SK 쉴더스

Threat Intelligence Report

EQST INSIGHT

EQST(이큐스트)는 'Experts, Qualified Security Team' 이라는 뜻으로
사이버 위협 분석 및 연구 분야에서 검증된 최고 수준의 보안 전문가 그룹입니다.

2025
07

SK 쉴더스

Contents

Headline

보안 가시성 확보와 틈새(Gray Zone) 해소 전략

Cloud 사업그룹 Cloud 보안컨설팅팀 백성광 팀장

■ 개요

우리는 변화의 시대를 넘어 '변혁의 시대'에 접어들었다. 1990 년대 인터넷의 시작은 시스템을 구축하고 서비스를 제공하는 과정 속에서 정보 유통과 소통의 폭발적 증가를 이끌었고, 우리는 이 서비스를 기반으로 다양한 정보를 주고받으며 현대인의 삶을 영위하고 있다.

서비스를 제공하는 기업들은 자체 데이터센터와 서버(On-Premise) 환경에서 IT 자원을 관리해 왔다. 그리고, 클라우드(Cloud) 시장의 성장과 기술의 발전으로 필요에 따라 IT 자원을 탄력적으로 사용할 수 있게 되면서, 클라우드를 도입해 업무와 서비스에 활용하고 있다. 최근에는 인공지능(AI) 기술이 급속히 발전하며 다양한 분야에서 AI 서비스를 접목하고 있다. 기업들은 경비절감 등 효율성 높이기 위해 인공지능(AI) 도입하고 있으며 정부 • 공공기관은 AI 역량확보와 경쟁력 강화를 위해 규제해왔던 망분리를 완화하고 개선하고 있다.(N2SF : National Network Security Framework, 금융분야 망분리 개선 로드맵)

■ 해커의 Target, 보안의 틈새(Gray Zone)

On-Premise 환경에서 Cloud 와 AI 기술로의 전환이 가속화되면서, 조직이 인지하지 못했던 보안 취약점이 발생하고 있다. 해커들은 이러한 틈새를 금전적, 군사적·정치적 목적 등 다양한 이유로 노리고 있다.

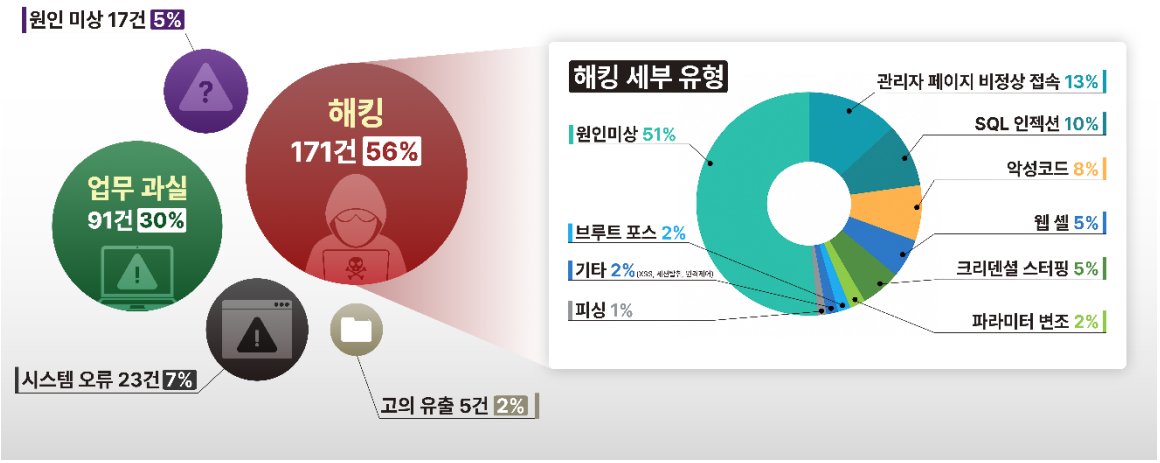
보안의 틈새(Gray Zone)는 관리되지 않고 방치된 자산, 위험관리 활동의 부재, 인적 실수 등으로 발생한다. 보안사고 사례를 보면, 그 원인은 대부분 VPN 등의 서비스 표면 취약점이나 웹 및 애플리케이션(Application) 취약점에 대한 식별 및 조치 부족, 또는 외부 인터넷 통제 미흡으로 업무용 사용자 PC 가 악성코드에 감염되면서 발생한 경우가 많았다.

기업들은 일부 IT 서비스를 클라우드를 통해 운영하는 추세이며, 이에 따라 많은 보안담당자들은 클라우드 영역에서의 보안 관리에 어려움을 호소하고 있다. 이는 개발 부서가 자체 승인만으로 클라우드 서비스를 사용할 수 있어 보안 부서가 이를 인지하지 못한 채, 보안성 검토가 이루어지지 않거나, 클라우드 환경에서 어떤 서비스의 어떤 기능을 확인하고, 발생하는 로그를 어떻게 관리해야 하는지에 대한 명확한 기준이 부족하기 때문이다. 마치 구름 속을 들여다보는 듯한, 보안 가시성이 확보되지 않은 회색지대(Gray Zone)를 노린 해킹 사고가 빈번히 발생하고 있다.

글로벌 헬스케어 랜섬웨어(UnitedHealth Group, Change Healthcare 등), Snowflake 클라우드 플랫폼 MFA 계정 탈취, Yes24 랜섬웨어 감염 등 일반 기업을 대상으로 금전적 목적의 보안사고가 지속적으로 발생하고 있다. 국가 간 분쟁의 경우, 우크라이나-러시아 전쟁(2022 년~현재)을 전후로 양국은 정부 및 금융기관 대상 DDoS(디도스) 공격, WhisperGate 등 데이터 와이퍼 악성코드 배포, 위성통신 해킹, 피싱 및 군사 데이터 탈취 등의 사이버 공격을 감행했으며, 이스라엘-하마스/이란 간 분쟁에서도 정부·언론 서비스를 향한 DDoS 공격과 전력망 운영사에 대한 해킹이 이루어졌다.

우리나라도 1953 년 휴전 이래 북한과의 대치가 지속되고 있으며, 사이버공간에서도 북한의 공격은 끊임없이 이어져 왔다. 7.7 디도스 공격(2009 년), 3.20 사이버 테러(금융사·방송사 해킹, 2013 년), 서울시 교통망·통신망 해킹 시도(2019 년), 한국수력원자력 공격(2020 년) 등 수많은 사이버 공격이 발생했다. 최근 발생한 S 통신사의 BPF 해킹 사건 또한 사이버 안보 위협의 일환으로 해석하는 시각이 많다. 아울러 중국-대만 간 갈등 고조에 따라, 미국의 전략적 거점인 우리나라를 겨냥한 사이버공격 시도도 더욱 증가할 것으로 예상된다.

해커의 공격방식은 다양하지만, 공격의 대상은 대부분 조직 시스템 내 존재하는 취약점에서 시작된다. 개인정보보호위원회가 2025 년 5 월 발표한 '개인정보 안전관리 체계 강화 추진 방향' 자료에 따르면, 지난해 국내 보안사고 중 56%가 시스템 취약점을 노린 해킹에 의해 발생한 것으로 나타났다.



* 출처 : 개인정보위 (2025.5.21)

그림 1. 지난해 개인정보 유출사고 원인유형

사이버 보안사고 관련 뉴스기사를 접하면 낯선 용어나 기술적인 설명으로 인해 이해가 어려울 수 있으나, 대부분은 시스템의 취약점을 통해 해킹이 발생하고, 정보가 유출된다는 내용이다. 해커들은 조직 내 가장 약한 고리, 즉 시스템의 취약점을 타깃으로 삼아 침투한다.

■ 보안의 틈새(Gray Zone) 찾고, 메꾸자

사람들은 건강한 삶을 통해 행복을 추구하며, 이를 위해 규칙적인 식사, 수면, 운동을 실천하려고 노력한다. 또한 정기적인 건강검진을 통해 자각하지 못한 질병을 조기에 발견·치료하여 건강을 유지한다.

조직의 튼튼한 사이버 보안을 위해서도 기본적인 활동이 필요하다. 보안의 기본은 보안 솔루션을 운영하고, 침해사고를 모니터링·대응하는 것, 보안 관리체계(Information Security Management System)를 마련하고 위험을 관리(Risk Management)하는 것이다. 그리고 기술 환경의 변화로 발생하는 보안의 틈새(Gray Zone)를 해소하기 위해서는 새로운 기술을 적용한 보안 전략이 필요하다.

1. 보안솔루션의 구축 및 운용

2000 년대 초반부터 많은 전문가들은 보안을 '성(Castle)'에 비유해 설명해 왔다. 조직 내부(내부망)와 외부(인터넷)를 명확히 구분하고, 외부의 위협을 차단하기 위해 방화벽, 침입탐지시스템(IDS), 침입방지시스템(IPS) 등 네트워크 경계에 방어체계를 구축하는 방식은 중세 성곽의 높은 성벽과 해자를 통해 침입을 막는 구조와 유사하다.

조직이 사이버 보안체계를 구축할 때 가장 먼저 고려해야 할 것은 보안 솔루션이다. 성벽을 세우고 성문에 경비를 배치해 출입을 통제하듯, 내부와 외부를 구분할 수 있는 방화벽을 구성하고, 외부에서 내부로 유입되는 위협을 탐지하고 차단하기 위해 WAF 및 IPS 등의 침입 차단 시스템을 구축해야 한다. 이후 내부 단말(PC) 통제, 시스템 접근 통제, 계정 관리, DB 암호화, 백업 및 복구 시스템 등을 구축함으로써 보안 활동의 기반이 마련된다.

해킹 사고는 취약점을 통해 침입한 후, 단말(PC, 서버)에서 정보 수집, 주변의 다른 취약한 시스템 검색, 악성코드/백도어 설치, 랜섬웨어 설치, 정보유출, 금전요구 등의 절차로 진행된다. 침입 후 설치되는 랜섬웨어 등 최근에 발생한 사고들의 지능화된 알려지지 않은 악성코드를 백신 등으로는 탐지하기 어려우므로 해당 악성 행위 탐지 및 대응이 가능한 EDR(Endpoint Detection & Response)의 도입은 기존 보안솔루션을 확인되지 않았던 회색지대(Gray Zone) 해소하고 가시성을 확보하는데 도움이 된다.

담당자의 경험 부족이나 조직의 비용 부족으로 인해 Cloud 에서도 회색지대가 다수 발생하고 있다. Cloud 인프라의 보안을 위해 방화벽, IPS, 접근제어, CloudTrail 을 이용한 로그모니터링 등을 적용하고 있지만, 조직에서 운영하고 있는 보안상태를 명확히 인지하기 어렵다. Cloud 서비스의 보안 가시성 확보를 위해 보안상태를 실시간으로 파악할 수 있는 CSPM(Cloud Security Posture Management)과 워크로드의 실행 환경 위협을 탐지·방어하고 취약점을 관리하는 CWPP(Cloud Workload Protection Platform) 솔루션이 필요하다. 또한, 각 보안 솔루션에서 발생한 보안 이벤트를 SIEM(Security Information and Event Management)을 통해 통합 수집하고, 이벤트 간 연관 분석을 통해 침해 시도를 식별하고 차단해야 한다. 보안 솔루션이 적용되지 않은 영역(예: 서버 접속 계정의 적정성 검토, 서비스 관리 페이지의 계정 권한 검토 등)은 인적 자원을 활용하여 기준과 절차에 따라 지속적으로 관리해야 한다.

2. 보안 관리체계 마련 및 위험관리 활동

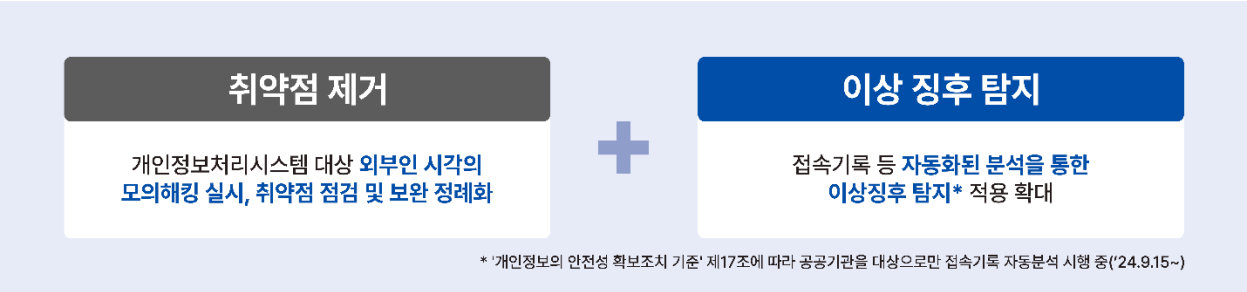
보안 솔루션을 통해 외부의 위협으로 부터 조직을 보호하는 성(Castle)을 쌓았다면, 이제는 이를 체계적으로 운영할 관리체계를 갖추어야 한다. 기준(규정)을 수립하고, 담당 조직을 구성하여 경비대장, 망루병, 경계병 등의 역할을 부여해 운영하는 것이다. 동시에 성곽, 수로, 해자 등의 방어 시설이 튼튼한지 수시로 점검하고 보수해야 한다.

사이버 보안도 마찬가지다. 내부 시스템과 정보 자산을 보호하기 위해 규정·지침·절차를 수립하고, 정보보호 기획, 솔루션 운영, 침해 대응, 보안 점검 등을 수행할 조직을 구성해야 한다. 연간 계획을 수립하고, 경영진의 승인 아래 주기적으로(연간/분기/월간/일간 등) 계획된 보안 관리를 실행해야 한다.

위험 관리 활동이란 보호해야 할 자산(시스템, 정보, 인력 등)을 식별하고, 알려진 취약점을 점검·제거·관리하는 것이다. 자산 식별에는 정보, 하드웨어, 소프트웨어, 시설, 인력 등이 빠짐없이 포함되어야 한다.

식별된 시스템에는 CCE(Common Configuration Enumeration), CVE(Common Vulnerabilities and Exposures) 등 알려진 취약점이나, 소스코드/웹/모바일 애플리케이션에 존재하는 취약점을 점검하고 제거해야 한다. 기능상 제거가 어려운 경우, 시스템 교체나 기능 개선 등의 계획을 수립하고, 접근 통제 및 사후 모니터링 등 보완 대책을 병행해야 한다.

신규 시스템 도입이나 변경이 발생할 경우, 자산 관리대장을 갱신하고 해당 시스템의 취약점을 제거하는 것이 가장 기본적이면서 중요한 절차다. 개인정보보호위원회는 '개인정보 안전관리 체계 강화 추진 방향'에서 취약점 제거를 보안의 최우선 과제로 제시하고 있다.



* 출처 : 개인정보위원회

그림 2. 추진과제: ①즉각적·기술적 조치사항(1)

최근 ISMS 인증을 받은 기업에서도 보안 사고가 발생하면서 "인증을 받았는데 왜 사고가 나느냐"는 질문을 받는 경우가 많다. ISMS-P(Information Security Management & Personal Information System)는 조직의 보안 활동을 구조화하기 위한 '틀'이며, 인증은 건강검진처럼 상태를 확인하고 부족한 부분을 개선하기 위한 과정이다.

건강하기 위해 잘 먹고, 잘자고, 열심히 운동하지만, 여러가지 주변 환경 등의 영향으로 병이 발생하고 건강이 악화되는 것처럼 매년 예방 측면에서 ISMS-P 인증 유지를 통해 매년 발견되는 보안관리 미흡한 부분과 취약점을 개선하면서 보안을 강화해야 한다.

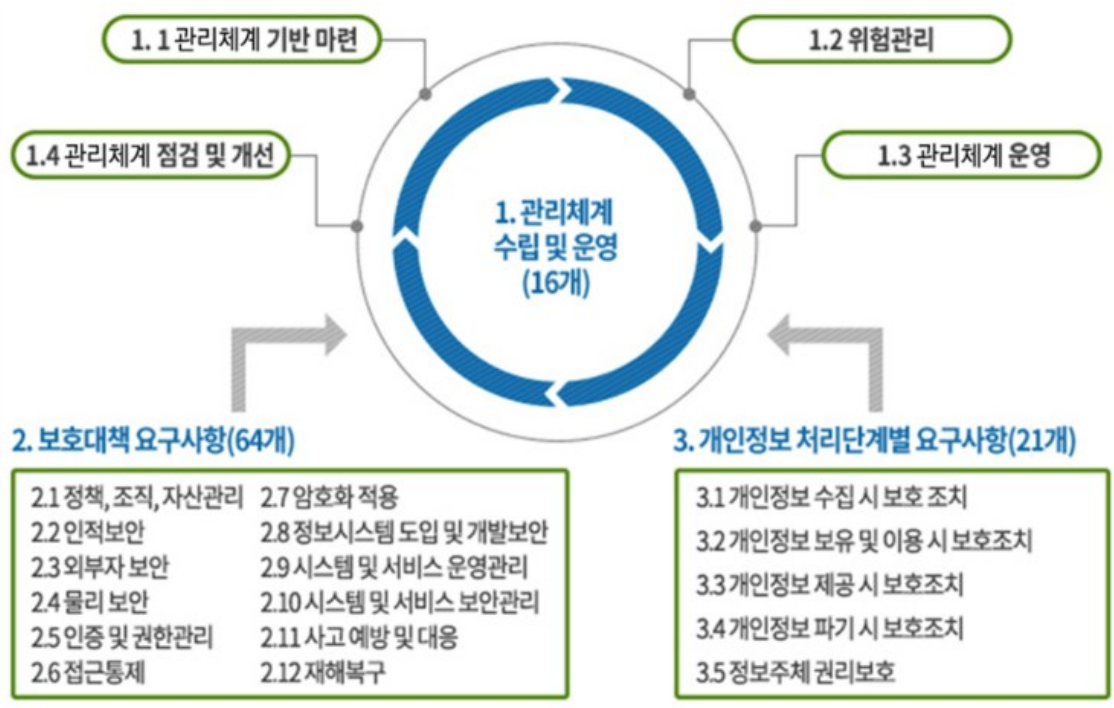


그림 3. 한국인터넷진흥원(KISA)홈페이지>ISMS-P 인증 제도 소개>인증기준

3. 보안의 틈새(Gray Zone)를 찾고 해소하다

이스라엘 역사상 가장 강력한 왕 다윗은 난공불락으로 여겨지던 예루살렘 성을 함락시켰다. 깊은 계곡으로 둘러싸인 산악 요새였지만, 외부에서 내부로 연결된 식수용 터널을 통해 성 내부로 침투했다. 강력한 성이 무너진 원인은 구조적·관리적 취약점이었다.

조직의 사이버 보안도 마찬가지다. 보안 솔루션과 ISMS-P 체계를 갖추고 매년 점검을 수행하더라도, 인지되지 못한 회색지대(Gray Zone)는 여전히 존재할 수 있으며 이것이 해커의 주요 타깃이 된다. 손자병법의 '지피지기 백전불태(知彼知己 百戰不殆)'처럼, 우리가 보호해야 할 시스템, 자산, 데이터 등을 명확히 파악하면 취약점을 제거하고 공격 노출을 줄일 수 있다. 더불어 최근 보안 사고의 유형과 공격 패턴을 분석하고, 해커의 시각에서 시스템을 점검한다면 회색지대를 효과적으로 해소할 수 있을 것이다.

ISMS-P 는 각 항목을 '적정/미흡'으로만 평가하므로 '충분히 안전한가'에 대한 정성적 평가는 어렵다. 따라서 보안성숙도 모델이나 MITRE ATT&CK 프레임워크*와 같은 기준을 병행해 운영하는 것도 효과적인 방법이다.

구분	CMMI	CMMC	C2M2
목적	조직의 프로세스 성숙도와 운영 효율성 개선	사이버보안 역량의 성숙도 평가 및 DoD 준수	IT/OT 사이버보안 역량 증진 및 위험 관리
적용 분야	업종 무관, 비즈니스 전반 (소프트웨어, 서비스 포함)	방위산업, DoD 계약/협력사 (FCI, CUI 취급 조직)	주요 기반시설(에너지, 통신 등) 및 모든 산업
구성 /범위	프로젝트/조직 전체 프로세스 영역 (최대 22 개)	17 개 보안 도메인/ 3~5 개 성숙도 레벨	10 개 도메인/350 개 이상 사이버보안 실천항목
성숙도 단계	5 단계(초기~최적화)	3~5 단계(Foundational~Expert, 버전에 따라 다름)	각 도메인별 4 MIL 단계 (MIL0~MIL3, C2M2 v2 기준)
평가 방식	공식 심사/외부 평가, 내부 개선/벤치마킹 목적	외부 감사(3rd-party), 자기평가 (저단계), DoD 요구사항	자기진단 및 외부 평가 병행, 도메인별 개별 측정
대표 특징	운영, 프로젝트, 서비스 전반의 프로세스 통합·최적화	NIST SP 800-171 연계, 보안 규정 준수, 법적 필수	실제 보안 실무, 조직 내/외부 위험관리, 인적·과정·기술 균형
필수성	선택(벤치마킹, 경쟁력 강화를 위한 국제 표준)	필수(방위산업/DoD 협력사는 반드시 준수)	선택(기반임계 산업군은 요구/권장)

표 1. 성숙도 모델 비교-프렉시티(Perplexity) 정리 자료

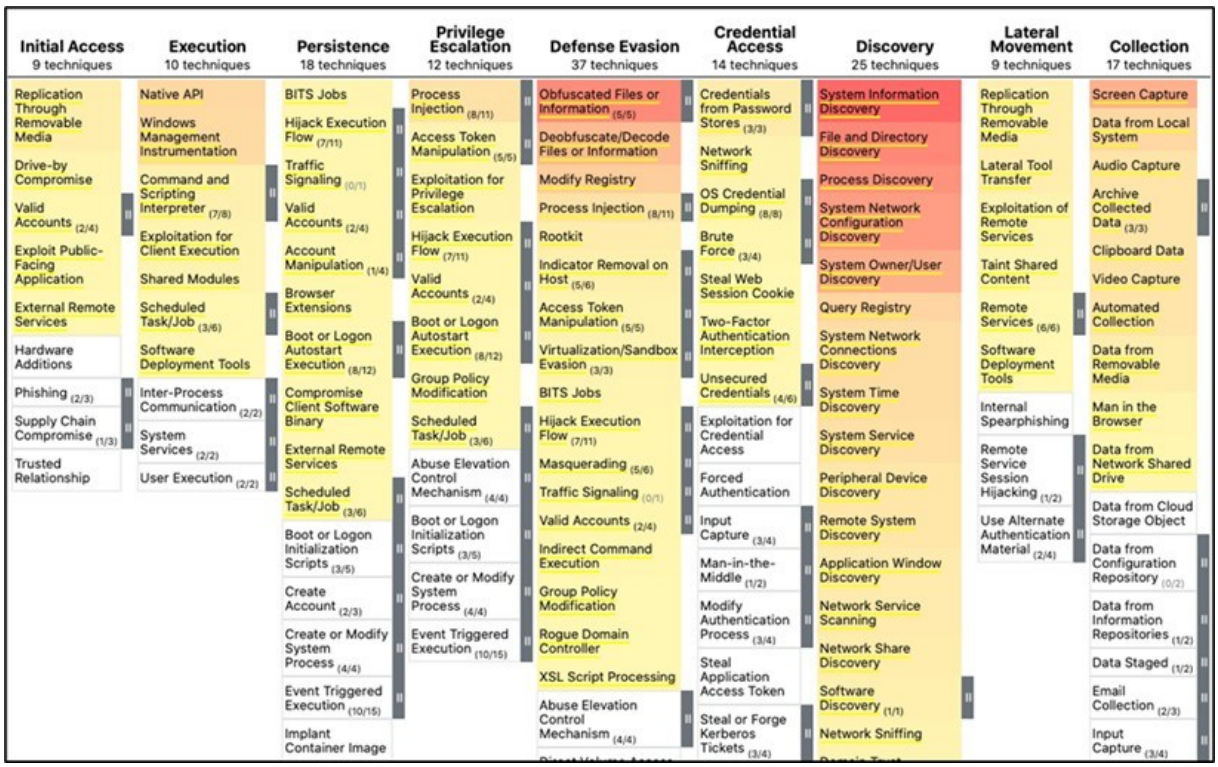


그림 4. MITRE ATT&CK Metrix - Navigator 중 일부 발췌

* MITRE ATT&CK 프레임워크 : MITRE ATT&CK는 Adversarial Tactics, Techniques and Common Knowledge의 약자로 공격자들이 실제로 사용하는 전술(Tactics), 기술(Techniques), 절차(Procedures)을 체계적으로 분류한 지식 기반 매트릭스이다.

마지막으로, 조직의 사이버 보안에도 분명한 '목표와 전략'이 필요하다. 목표가 없다면 보안의 일관성과 실행력을 확보하기 어렵다. 목표는 위험 완화와 자원 우선순위를 결정하는 기준이 되며, 보다 효율적이고 효과적인 보안 운영을 가능하게 한다.

보안 전략은 중장기 계획 또는 마스터플랜을 통해 수립된다. 과거에는 기업들이 보안 방향을 설정하고 실행 가능한 활동을 담은 마스터플랜을 마련했지만, 현재는 ISMS 인증이나 솔루션 도입으로 대체되는 경우가 많다. 그러나 종합적이고 효과적인 사이버 보안 체계를 운영하기 위해 마스터플랜은 여전히 필요하다.

■ 시사점

기술 발전, 범죄 양상, 국제 정세 변화에 따라 해커들은 끊임없이 우리 조직의 사이버 보안 회색지대(Gray Zone)를 노리고 있다.

보안 솔루션의 도입과 운영, 보안 체계 관리 및 위험 관리 등 기본적인 보안 활동을 통해 회색지대를 지속적으로 방어하고, 클라우드(Cloud) 및 인공지능(AI) 등 신기술 영역에서 보안 가시성을 확보하며, 조직 차원의 보안 목표를 수립하고 실행해 나간다면 해커의 공격과 사고로부터 조직의 사이버 안전 수준을 지속적으로 강화할 수 있을 것이다.

■ 참고 문헌

[1] 개인정보위원회, (별첨2) 개인정보 정책포럼 발표자료(개인정보 유출사고 현황 및 대응방향)

[2] KISIA, 2024년 국내 정보보호산업 실태조사 보고서

[3] 보안성숙도 모델을 활용한 정보보호 관리수준 점검 방법에 관한 연구_고려대학교 이상규

■ 참고 자료

[1] 한국인터넷진흥원, ISMS-P인증 제도소개

[2] SK쉴더스, 위협 중심 보안 전략의 핵심 도구: Rule Framework

Keep up with Ransomware

피해자별 협상 채널 구축하는 DireWolf 랜섬웨어

■ 개요

2025 년 6 월 랜섬웨어 피해 사례 수는 지난 5 월(484 건)에 비해 소폭 증가한 505 건을 기록했다. 4 월 이후, 대형 랜섬웨어 그룹들의 해킹 피해와 활동 중단 사례가 잇따르고 있다. 이에 반해 한두 달간 짧게 활동하는 신규 랜섬웨어 그룹의 비중이 증가하는 추세다. 지속적인 법 집행 기관의 단속과, 피해 기업들의 몸값 지불 거부 등으로 장기 활동에 대한 부담이 커진 것으로 보인다. 따라서 랜섬웨어 그룹들은 서비스 형태의 랜섬웨어를 활용해 단기간에 집중적으로 활동하거나, 하나의 조직이 여러 랜섬웨어 프로젝트를 진행하는 경우, 그리고 리브랜딩을 통해 수시로 정체를 바꾸는 경향이 뚜렷해지고 있다.

이러한 흐름을 뒷받침하는 한 예로, Hunters 그룹이 7 월 초 공식적으로 랜섬웨어 활동 중단 선언을 했다. 7 월 3 일, 자신들의 다크웹 유출 사이트의 공지사항으로 "Hunters International 프로젝트를 종료하기로 결정했습니다." 라는 내용을 전달하며, 자신들의 행동이 미치는 영향을 잘 알고 있고 선의의 표시로 복호화 도구를 무료로 배포하겠다고 발표했다. 하지만 복호화 도구는 아직 공개되지 않았으며, 다크웹 유출 사이트에 모든 피해 기업 및 유출 데이터만 내려간 상태이다. 이들의 프로젝트 종료 움직임은 지난 24 년 11 월부터 있었다. Hunters 를 이용하는 제휴사의 패널에 랜섬웨어 프로젝트는 위험성이 높으나 수익성은 점점 낮아지고 있어 랜섬웨어 프로젝트를 종료할 것이라는 글을 업로드 했으며, 지난 1 월에는 데이터 탈취 만을 목적으로 하는 신규 프로젝트 World Leaks 를 내부적으로 공개하기도 했다. 이후 지난 5 월부터 World Leaks 활동을 시작했으며, 7 월에는 Hunters 프로젝트를 공식적으로 종료했다.

사이버 범죄 인프라 전반에서도 유의미한 변화가 이어지고 있다. 대표적인 해킹 포럼 중 하나인 BreachForums 의 주요 운영진들이 지난 2 월과 6 월에 프랑스 사이버 범죄 수사 부서(BL2C)에 체포되며, 포럼이 잠정 폐쇄된 것으로 확인됐다. 해킹 포럼 RaidForums(15 년 개설)을 대체하기 위해 2022 년에 만들어진 BreachForums 는 설립 이후에도 지속적으로 법 집행 기관의 감시를 받아왔다. 23 년에는 운영자 pompompurin 이 FBI 에 체포되어 사이트가 압수되었으며, 이어 24 년에 운영자 Baphomet 이 체포되면서 다시 폐쇄된 바 있다. 이후 포럼은 25 년 4 월에 다시 한번 폐쇄됐는데, 당시 운영진은 BreachForums 에서 사용하는 오픈 소스 포럼 소프트웨어 MyBB 의 제로데이 취약점을 통해 법 집행 기관이 접근할 수 있어, 포럼을 임시로 비활성화 한다고 설명했다. 발표에 따르면, BL2C 는 올해 2 월 주요 관계자 중 한명인 IntelBroker 를 체포했으며, 6 월에는 ShinyHunters, Hollow, Noct, Depressed 등 핵심 인물 4 명을 추가로 검거했다. 이 일련의 체포로 포럼 운영에 타격을 입으면서 BreachForums 는 현재까지도 운영되지 않고 있다. 다른 운영자들은 7 월에 BreachForums 복구를 예고했지만, 현재까지 공식적으로 복구된 사이트는 확인되지 않고 있다.

기존 그룹들의 활동 중단과 사이버 범죄자들의 체포 소식이 이어지는 가운데, 파트너를 모집하며 활동을 준비하는 그룹들도 확인됐다. 4 월에 RaLord 라는 이름으로 등장 후 5 월에 리브랜딩한 Nova 그룹이 6 월에는 RAMP 포럼에 홍보글을 업로드하며 활동에 박차를 가하고 있다. 기존에 자신들의 다크웹 유출 사이트에서 홍보하던 제휴 서비스는 물론이고, 랜섬웨어 기능을 상세하게 소개하며 랜섬웨어 서비스를 이용할 파트너를 모집하고 있다. 21 년부터 활동하고 있던 Chaos 그룹도 본격적으로 홍보를 시작했다. 이들은 별도의 다크웹 유출 사이트가 없이 활동하다가 25 년 4 월부터 다크웹 유출사이트도 운영하기 시작했으며, 6 월에는 RAMP 포럼에 홍보글을 게시하며 함께 일할 인원을 모집하고 있다. 그 외에도 6 월에 새로 등장한 WarLock 그룹도 RAMP 포럼에 새로운 파트너를 모집하는 글을 게시했으나, 현재 다크웹 유출 사이트에 접속이 불가능한 상태이다.

올해 상반기 기준 Clop 에 이어 다크웹에 두번째로 많은 피해자를 게시한 Qilin 그룹(333 건)이 5-6 월에 진행한 랜섬웨어 공격에 보안업체 Fortinet 의 보안 장비의 운영체제(FortiOS)의 취약점을 악용한 것으로 확인됐다. 공격에 사용된 취약점은 원격 코드 실행 취약점인 CVE-2024-21762 와 인증 우회 취약점 CVE-2024-55591 로, 두 취약점 모두 이미 패치가 배포된 상태다. 그러나 Qilin 은 여전히 패치되지 않은 취약한 시스템을 노리며 공격을 수행하고 있다. 이처럼 공격자들은 보안 업데이트가 적용되지 않은 취약한 시스템을 주요 표적으로 삼기 때문에, 소프트웨어와 보안 장비의 정기적인 패치 적용이 필수적이다

■ 랜섬웨어 뉴스

Hunters International, 랜섬웨어 프로젝트 종료

- 7월 3일 자신들의 DLS를 통해 랜섬웨어 활동을 종료한다고 공식적으로 발표
- 피해 기업과 모든 데이터는 DLS에서 더 이상 접근 불가능하며, 피해 기업에게 무료로 복호화 도구 배포 예정
- 내부적으로는 지난 1월부터 랜섬웨어 프로젝트 대신 데이터 탈취 프로젝트로 전환을 준비
- 해당 프로젝트는 5월에 등장한 World Leaks

BreachForums 주요 관계자 체포 및 운영 중단

- 지난 2월 프랑스 사이버 범죄 수사 부서(BL2C)에 의해 IntelBroker 체포
- 6월에는 ShinyHunters, Hollow, Noct, Depressed 등 핵심 인물 4명 추가로 체포
- BreachForums는 지난 4월 MyBB 취약점으로 법 집행 기관이 접근할 수 있다며 사이트를 잠정 폐쇄
- 7월에 복구 예정이라 하였으나, 공식적으로 복구된 사이트는 확인되지 않음

Fortinet 취약점을 악용한 Qilin 그룹

- Qilin 그룹은 지난 5-6월 공격에 FortiOS의 취약점을 악용
- 사용한 취약점은 원격 코드 실행 취약점(CVE-2024-21762)과 인증 우회 취약점(CVE-2024-55591)
- 두 취약점 모두 패치가 배포됐지만, 아직 적용하지 않은 시스템을 표적으로 공격

신규 WarLock 그룹, DLS 소스코드에 한국어 발견

- 러시아 해킹 포럼 RAMP에 홍보글을 업로드하며 그룹 공개
- 공개 이전부터 피해자가 다수 게시된 것으로 보아, 6월 이전부터 활동한 것으로 추정
- 공개한 DLS에 한국어로 된 주석 발견


BlackLock과 Global 간의 연관성 확인
이전에 El Dorado, Mamona R.I.P를 운영한 BlackLock 그룹이 Global도 운영하는 것으로 추정
6월에 발견된 Global 그룹의 랜섬노트에 BlackLock DLS 포함
BlackLock의 운영자 $$$가 RAMP 포럼에 Global 홍보글 게시
다양한 신규 그룹의 등장
Akira의 DLS에 사용된 문구, 색상, 기능을 모방한 Kawa4096 그룹
협상중이거나 기한을 넘기지 않은 피해자명을 필터링해 업로드하는 W.A. 그룹
그 외 TeamXXX, Nemesis 그룹도 새롭게 등장

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

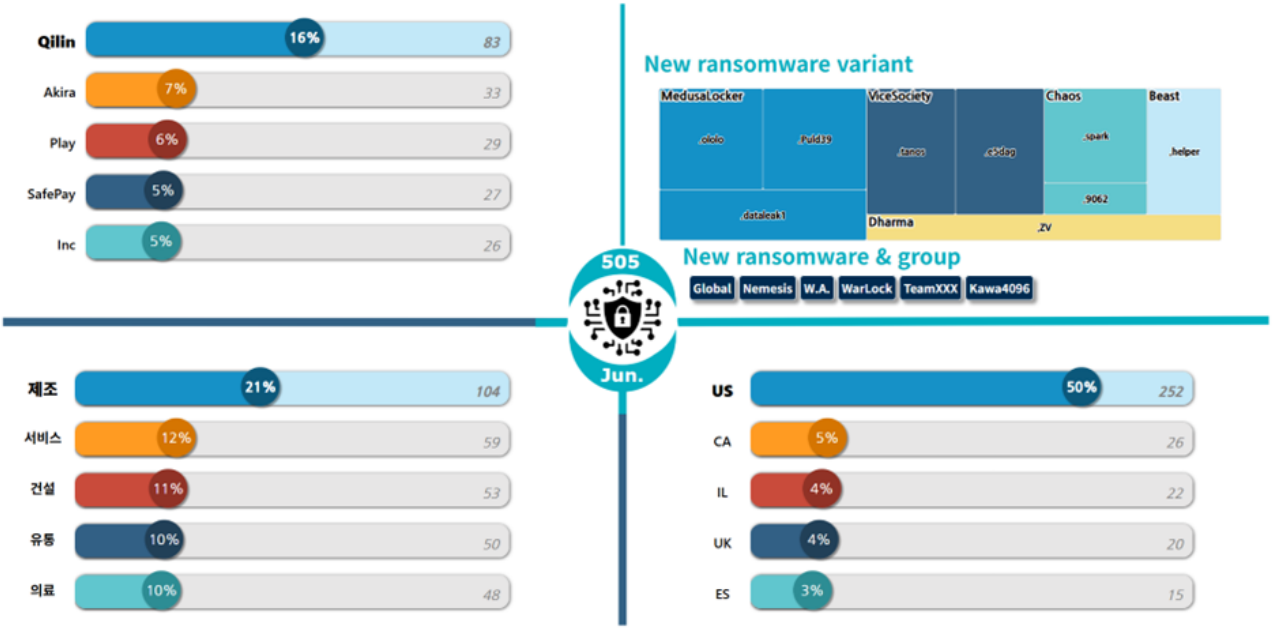


그림 2. 2025 년 6 월 랜섬웨어 위협 현황

새로운 위협

6 월에는 총 5 개의 신규 랜섬웨어 그룹이 등장했으며, 1 개의 그룹이 리브랜딩 후 활동을 재개했다. 신규 그룹 TeamXXX 는 6 월에 피해자 8 건을 게시했으며, 신규 그룹 W.A. 는 4 건을 게시했다. 특히 W.A. 그룹은 협상을 진행중이거나 아직 비용 지불 기한을 넘기지 않은 피해 기업의 이름을 필터링해 업로드하며, 협상에 실패하거나 기한을 넘기면 데이터와 기업명을 공개하는 모습을 보인다.

```
159            title: '!!import',
160        html: 'In order to ensure communication efficiency, please contact us via Tox; we will no longer be resp
12px;">3DCE1C43491FC92EA7D10322040B254FDD2731001C2DDC2B9E819F0C946BDC3CD251FA3B694A</span><br><b>QtoxID(2)</b>:<
12px;">F79A71AD8BB2E3E7EDFC38970FDC05E922E429B5DFC325C7D0E91F216DE8F3537C1A1C97F197</span>',
161        icon: 'info',
162            confirmButtonText: 'ok'
163        });
164        // 클라이언트 데이터 로드 함수
165        async function loadClients() {
166            console.log("loadClients called");
```

그림 3. WarLock DLS 페이지 소스코드

신규 그룹 WarLock 은 운영자로 추정되는 유저 cnkjasdfgd 가 러시아 해킹 포럼 RAMP 에 홍보글을 업로드하며 발견됐다. 이미 다크웹 유출 사이트에는 여러 피해자가 게시되어 있어 실제 활동을 6 월 이전부터 했을 것으로 추정된다. 또한 다크웹 유출 사이트 소스코드에 한국어로 된 주석이 달려있었으나, 현재는 폐쇄되어 접근이 불가능한 상태이다.

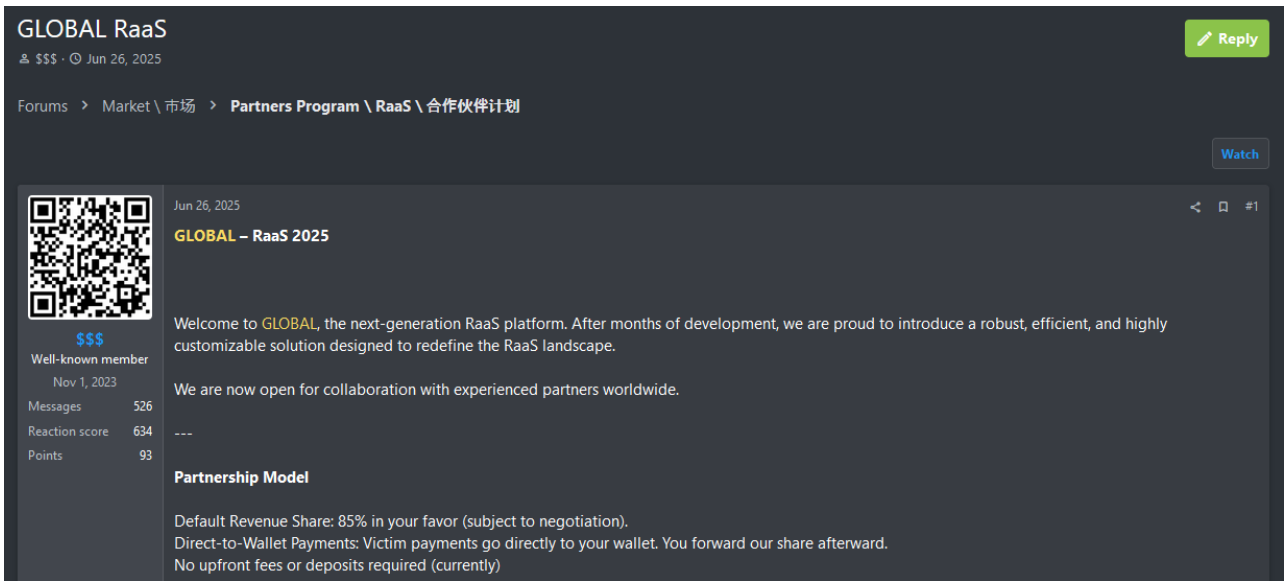


그림 4. Global RaaS 홍보글

신규 Global 그룹은 BlackLock 과 연관이 있는 것으로 확인됐다. 우선 6 월 초, BlackLock 의 또 다른 프로젝트였던 Mamona 랜섬웨어와 거의 동일한 버전의 Global 랜섬웨어가 발견됐다. 해당 랜섬웨어의 랜섬노트에 따르면 자신들을 Global 이라고 지칭하고 있지만, 랜섬노트에는 BlackLock 의 다크웹 유출 사이트 주소가 기재되어 있었다. 또한 협상 채팅에서는 Global 그룹의 다크웹 유출 사이트에서 피해 사실을 확인할 수 있다고 언급했다. 비슷한 시기에 BlackLock 의 운영진 $$$ 는 RAMP 에 작성했던 BlackLock 홍보 글과 프로필에서 BlackLock 대신 Global BlackLock 으로 명칭을 변경했으며, 6 월 말에는 $$$ 가 Global RaaS 를 직접 홍보하는 글을 업로드 하며 BlackLock 과 Global 의 연관성이 확인됐다.

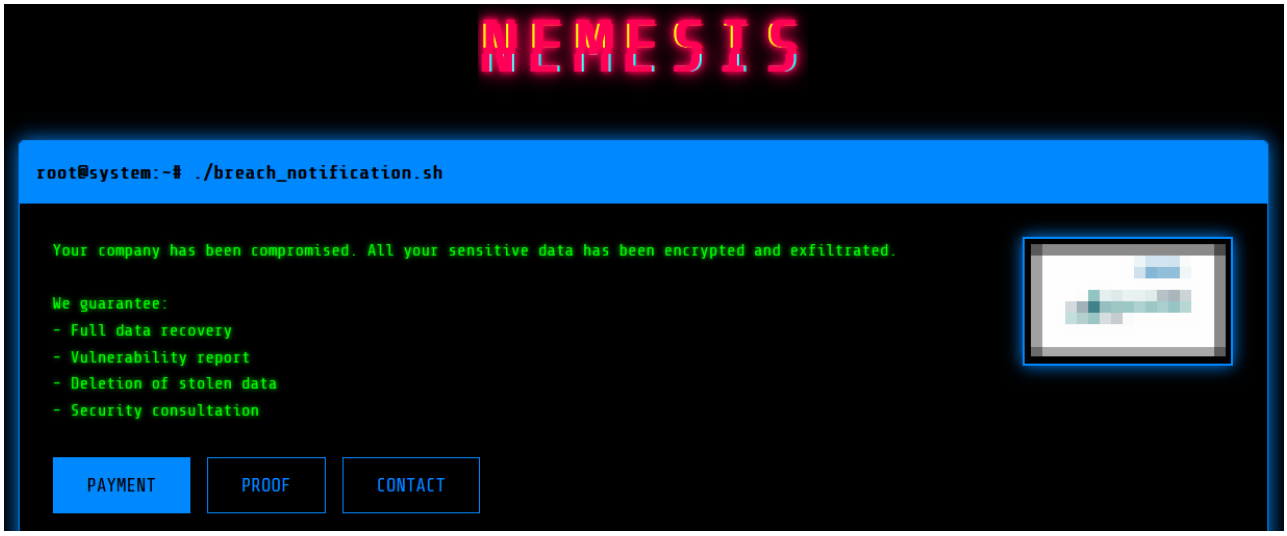


그림 5. Nemesis 협상 페이지

Nemesis 그룹은 탈취한 데이터를 공개하는 페이지는 아직 확인되지 않았다. 협상을 위한 채팅 페이지만 존재하거나, 피해자 및 유출 데이터를 한 곳에 모아 볼 수 있는 페이지가 있는 다른 그룹과는 달리, 랜섬노트에 피해자별로 별도의 토큰이 추가된 다크웹 페이지로 유도하고 있다. 이후 자신들이 탈취한 데이터의 샘플을 보여주고, 원하는 금액과 협상을 위한 메신저 ID 를 제공해 협상을 진행하고 있다.

그림 6. 다크웹 유출 사이트(상: Akira, 하: Kawa4096)

신규 Kawa4096 그룹의 다크웹 유출 사이트는 Akira 그룹의 다크웹 유출 사이트와 매우 유사한 디자인을 가지고 있다. 사용된 문구와 컬러는 물론이고, 콘솔 창처럼 보이는 디자인에 명령어를 직접 입력해야 다른 데이터에 접근할 수 있는 방식 등 많은 부분에서 유사점을 보이고 있다. 다만, 그룹 간에 직접적인 관계나 연관성이 없더라도 다크웹 유출 사이트의 디자인이나 문구 등을 모방하는 사례는 드물지 않기 때문에 두 그룹간의 관계를 더 지켜볼 필요가 있다.

Top5 랜섬웨어

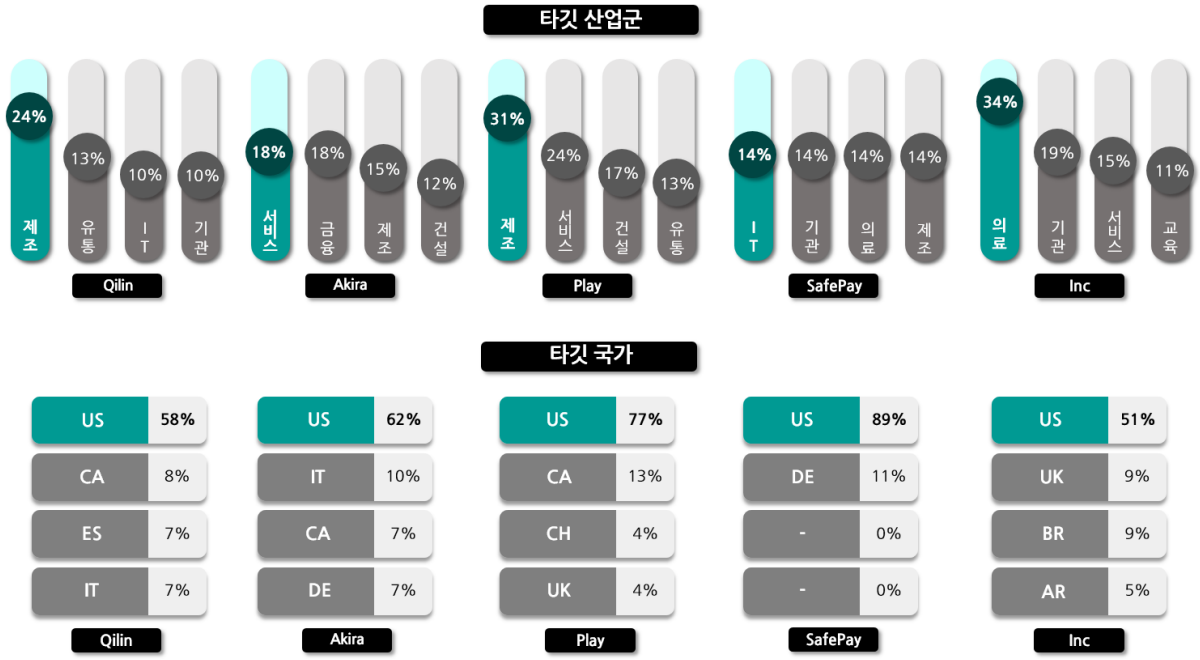


그림 7. 산업/국가별 주요 랜섬웨어 공격 현황

Qilin 그룹은 6 월 24 일 미국의 의료기관 Covenant Health 를 공격해 내부 문서를 유출했다. 유출된 자료에는 환자 의료 정보, 계약서, 세금 문서, 직원을 식별할 수 있는 파일 등이 포함됐다. 또한 6 월 23 일 미국 물류업체 Estes Forwarding Worldwide 가 공격당했으며, 여권 스캔본, 운전면허증, 직원 정보 스프레드시트 등이 샘플로 다크웹에 게시됐다. 영국의 스프링 제조업체 Airedale Springs Ltd.도 6 월 말 공격을 받아 내부 운영 문서, 공급망 관련 문서가 일부 유출됐다.

Akira 그룹은 6 월 초 미국의 사교 클럽 Sleepy Hollow Country Club 을 공격해 약 14GB 가량의 내부 데이터를 탈취했다. 이들은 6 월 말 모든 데이터를 공개했으며, 데이터에는 직원의 여권, 주민번호와 같은 개인정보는 물론 계약서, 재무제표 등이 포함되어 있다. 또한 아웃소싱 기업 Datrose 를 공격해 약 5GB 의 데이터를 탈취했다. 여기에는 이메일, 주소 등이 포함된 개인정보와 비밀 유지 계약서, 재무제표 등이 포함된 것으로 확인됐다.

Play 그룹은 미국 펜실베이니아의 운송업체 S&H Express 를 공격해 데이터를 탈취했다. 유출된 샘플에는 계약서, 고용 관련 문서, 세금 파일, 운전면허증 사본 등이 포함되었다. 또한 6 월 27 일 캐나다의 통신 장비 유통 기업 Cartel Communication Systems 도 공격을 받아 고객 명단, 내부 프로젝트 문서, 공급사 계약서, 일부 기술 문서가 다크웹에 게시됐다.

SafePay 그룹은 미국 오하이오주 Liberty Township 교육청을 공격해 일부 내부 재무자료, 운영 문서, 교직원 관련 문서가 포함된 48GB 의 데이터를 탈취했다. 또한 독일의 IT 서비스업체 MCSL GmbH 도 공격을 받아 고객 보고서, 프로젝트 문서, 내부 커뮤니케이션 파일이 유출되었으며, 미국의 차고 문 제조업체 The Overhead Door Company 역시 공격을 당해 기술 문서, 회계 기록, 고용 계약서 등이 포함된 내부 자료가 노출됐다.

Inc 그룹은 독일의 통신기기 제조업체 funktel GmbH 의 3.5TB 가량의 데이터를 탈취했다고 주장하며, 주요 제품의 설계도, 내부 메일, 급여 명세서, 운영 계획서 등 다양한 문서를 샘플로 공개됐다. 또한 미국의 의료 업체 Medical Center of Marin 을 공격해 환자 개인정보가 포함된 설문지나 의료 소견서, 환자의 신분증 등 환자의 정보가 유출됐다.

■ 랜섬웨어 집중 포커스

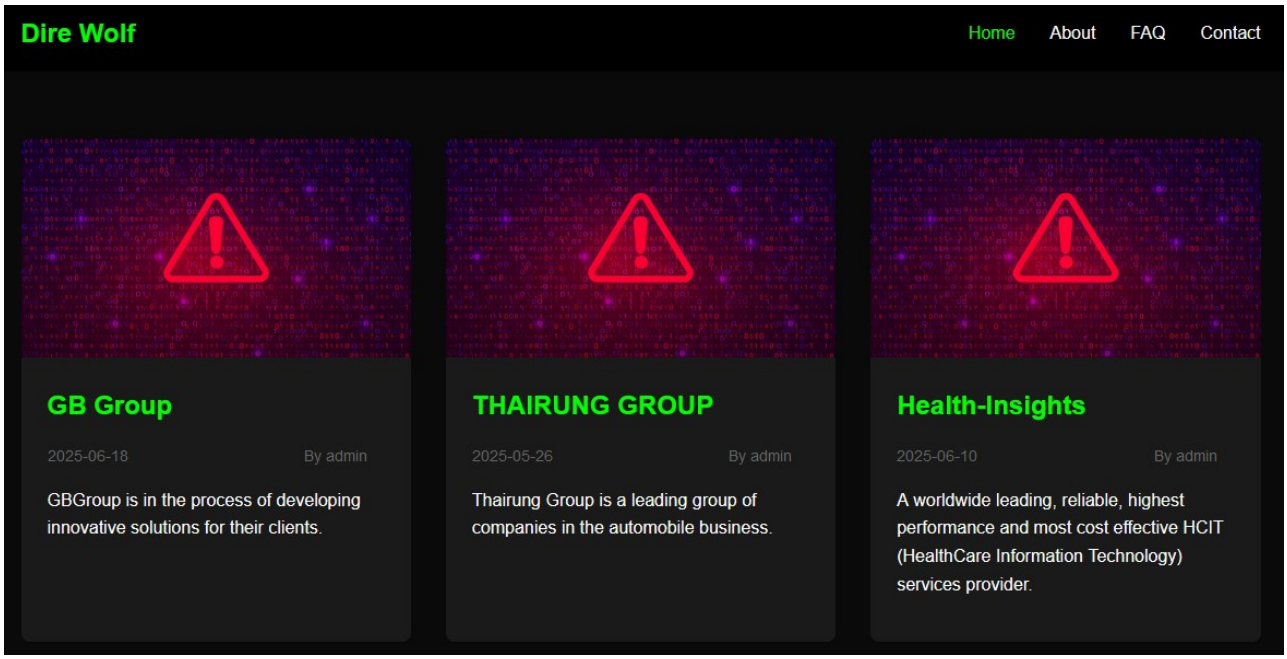


그림 8. DireWolf 다크웹 유출 사이트

25 년 5 월부터 활동을 시작한 DireWolf 그룹은 지금까지 총 16 건의 피해자를 게시했다. 각 피해자 마다 어떤 파일을 탈취했는지, 언제 업로드 했는지를 기록한 뒤, 협상에 실패하거나 일정 기간이 지나면 모든 사용자가 접근할 수 있도록 다크웹에 게시하고 있다.

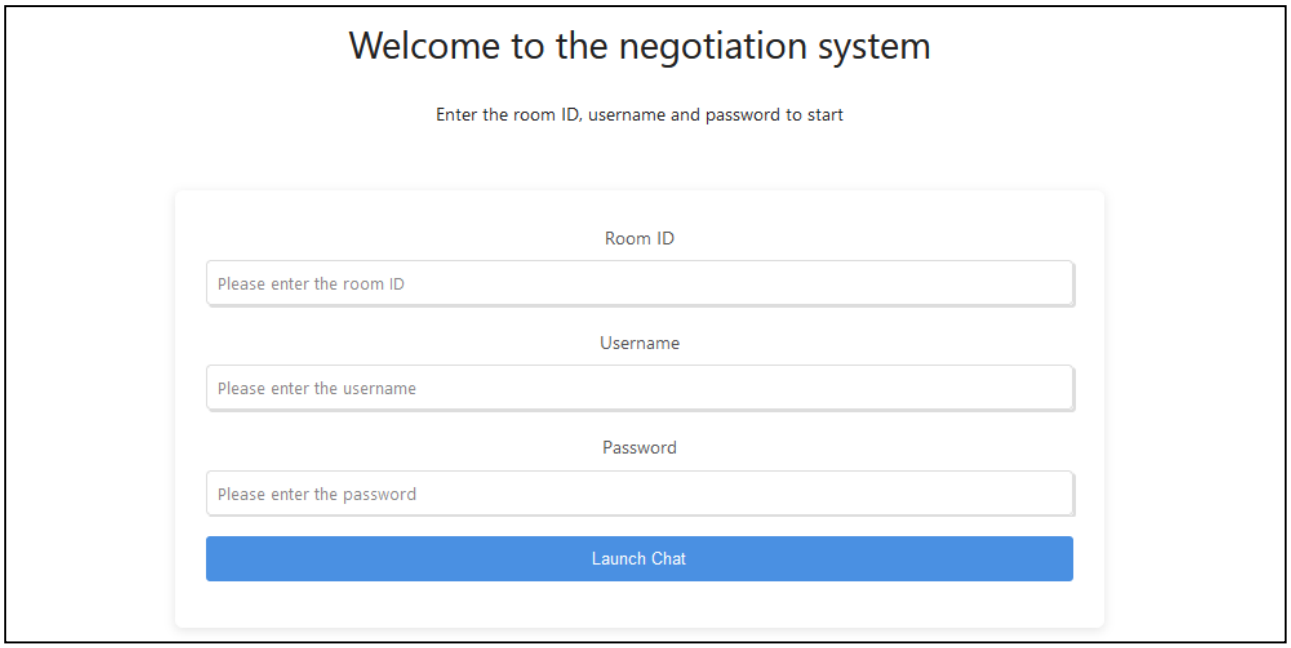


그림 9. DireWolf 다크웹 협상 페이지

랜섬노트에는 위 다크웹 유출 사이트 주소는 물론, 협상을 진행할 다크웹 채팅 사이트 주소와, 접속에 필요한 Room ID, Username, Password 를 함께 제공한다. 또한 자신들이 데이터를 탈취했음을 증명하기 위한 샘플 데이터를 다크웹에 업로드하는 것이 아니라, 이를 압축해 클라우드 스토리지 GoFile에 업로드하고 그 링크를 랜섬노트에 첨부해 피해자만 확인할 수 있도록 한다.

샘플 데이터가 업로드된 클라우드 링크를 제공하는 점과, 협상 페이지에 접속하기 위한 정보를 전달하는 점으로 미루어 보아, 이들은 각 피해자 별로 일부 수정된 랜섬웨어를 배포하고 있을 확률이 높다. 단순히 랜섬노트 내용만 변경한 뒤 배포할 수 있으며, 그 외의 기능도 맞춤으로 수정해 배포하고 있을 수 있다. 현재는 1 개의 피해자를 대상으로 하는 랜섬웨어만 확인됐으며, 이를 분석한 내용을 공유해 앞서 다가올 랜섬웨어 위협에 쉽게 준비할 수 있도록 하고자 한다.

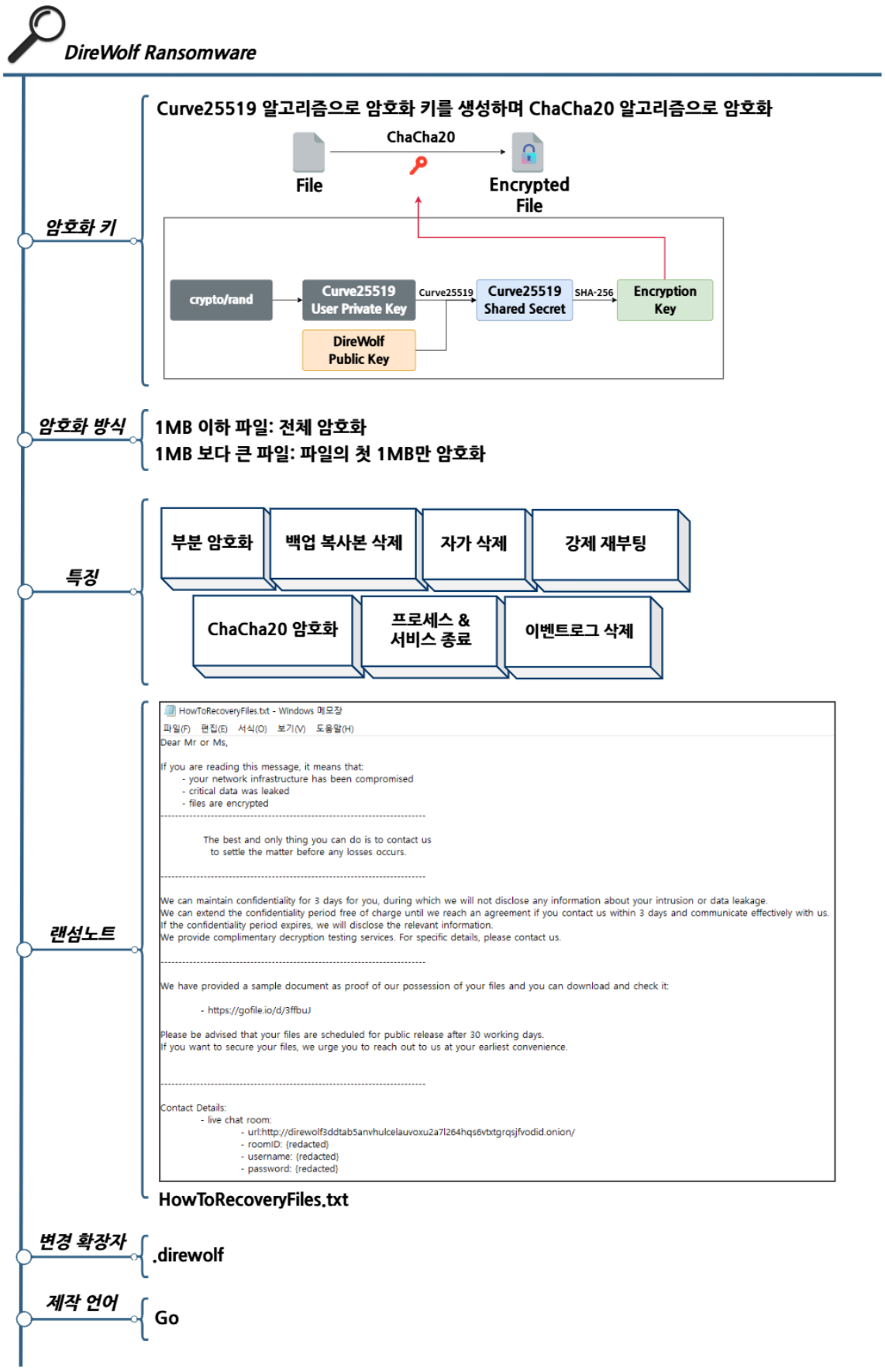


그림 10. DireWolf 랜섬웨어 개요

DireWolf 랜섬웨어 전략

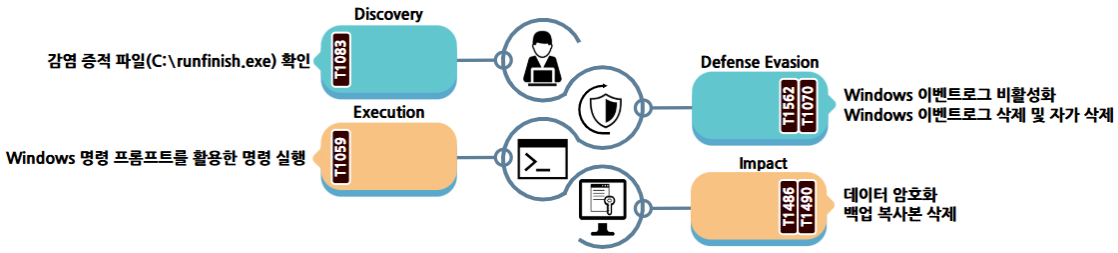


그림 11. DireWolf 랜섬웨어 공격 전략

DireWolf 는 별도의 설정 파일이 없으며, 2 개의 실행 인자를 사용해 기능을 제어할 수 있다. -h 인자를 사용해 실행 인자 설명을 볼 수 있으며, -d 인자를 사용해 특정 디렉터리만 암호화하도록 설정할 수 있다.

구분	설명
-h	실행 도움말 출력
-d <path>	특정 경로만 암호화

표 1. DireWolf 실행 인자

DireWolf 는 중복으로 실행되는 것을 방지하기 위해 뮤텍스[1] 를 활용한다. 랜섬웨어가 실행되면 “Global\direwolfAppMutex”라는 이름으로 뮤텍스를 생성하고, 이를 종료 직전에 해제한다. 만약 동일한 뮤텍스가 이미 생성되어 있다면 동일한 랜섬웨어가 이미 실행 중이므로 현재 프로세스를 종료해 중복 실행을 방지한다. 또한 DireWolf 랜섬웨어는 대상 시스템을 모두 암호화한 뒤 C:\runfinish.exe 경로에 빈 파일을 생성하는데, 랜섬웨어 시작 시 해당 파일이 존재하는지 확인해 이미 암호화된 시스템을 중복으로 탐색하고 암호화하는 것을 차단한다. 만약 뮤텍스나 runfinish.exe 파일이 존재하는 경우, 랜섬웨어 종료는 물론 아래 명령어를 사용해 자가 삭제를 진행한다.

```
cmd /C timeout /T 3 & del /f /q <path> & exit
```

표 2. 자가 삭제 명령어

자가 삭제 외에도 복구 방지는 물론 분석 방해와 탐지 회피를 위해 각종 기록이나 흔적을 삭제한다. 실행중인 Windows 이벤트 로그 프로세스는 종료하고, Windows 환경의 기본 이벤트 로그를 삭제한다. 또한 명령 프롬프트를 활용해 백업 복사본 삭제는 물론 복구 환경 비활성화나 복구 모드 진입 방지도 함께 진행한다.

[1] 뮤텍스(Mutex): 여러 프로세스 혹은 스레드가 동일한 자원을 동시에 접근하지 못하도록 하는 보호 기법

명령어	설명
Get-WmiObject -Class win32_service -Filter "name = 'eventlog'" | select -exp ProcessId exp ProcessId	이벤트 로그 프로세스 ID 확인
Get-WmiObject -Class win32_service -Filter "name = 'eventlog'" | select -	이벤트 로그 프로세스 ID 확인
taskkill /f /pid <PID>	이벤트 로그 프로세스 종료
vssadmin delete shadows /all /quiet	복원 지점 제거
wmic shadowcopy delete /nointeractive	복원 지점 제거
wbadmin stop job -quiet	실행중인 백업 작업 중단
wbadmin disable backup -quiet	예약된 백업 작업 중단
wbadmin delete backup -keepVersions:0 -quiet	모든 백업 버전 삭제
wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0 -quiet	시스템 상태 백업 삭제
wbadmin delete catalog -quiet	백업 메타데이터 삭제
bcdedit /set {default} recoveryenabled No	복구 환경(WinRE) 비활성화
bcdedit /set {default} bootstatuspolicy ignoreallfailures	복구 모드 진입 방지
wevtutil cl Application	Application 로그 삭제
wevtutil cl system	System 로그 삭제
wevtutil cl security	Security 로그 삭제
wevtutil cl setup	Setup 로그 삭제

표 3. 백업 및 이벤트 로그 삭제 명령어

원활한 파일 암호화를 위해 특정 프로세스와 서비스를 우선적으로 종료한다. 종료 대상 프로세스 및 서비스는 아래 표와 같다.

프로세스
wxServerView.exe, sqlmangr.exe, RAgui.exe, supervise.exe, Culture.exe, Defwatch.exe, httpd.exe, wsa_service.exe, synctime.exe, vxmon.exe, sqlbrowser.exe, memtas.exe, tomcat6.exe, Sqlservr.exe, agntsvc.exe, dbeng50.exe, dbsnmp.exe, dbsrv12.exe, encsvc.exe, excel.exe, firefox.exe, vss.exe, infopath.exe, isqlplussvc.exe, msaccess.exe, mspub.exe, mydesktopqos.exe, mydesktopservice.exe, ocautoupds.exe, ocomm.exe, ocssd.exe, onenote.exe, oracle.exe, outlook.exe, powerpnt.exe, sqbcoreservice.exe, sql.exe, steam.exe, tbirdconfig.exe, thebat.exe, thunderbird.exe, visio.exe, WinSAT.exe, winword.exe, wordpad.exe, onedrive.exe, wrapper.exe, xfssvccon.exe, sqlservr.exe, sqlagent.exe, sqlwriter.exe, MSExchangeIS.exe, MSExchangeTransport.exe, MSExchangeMailboxAssistants.exe, MSExchangeRepl.exe, MSExchangeRPC.exe, MSExchangeServiceHost.exe, notepad++.exe, notepad.exe

표 4. 종료 대상 프로세스

서비스
AcrSch2Svc, backup, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, BackupExecVSSProvider, CAARCUpdateSvc, CASAD2DWebSvc, ccEvtMgr, ccSetMgr, DefWatch, GxBlr, GxCIMgr, GxCVD, GxFWD, wuauserv, GxVss, Intuit.QuickBooks.FCS, memtas, mepocs, PDVFSService, QBCFMonitorService, QBFCService, QBIDPService, RTVscan, SavRoam, sophos, sql, stc_raw_agent, veeam, VeeamDeploymentService, VeeamNFSSvc, VeeamTransportSvc, VSNAPVSS, vss, YooBackup, YooIT, zhudongfangyu, SQLPBDMS, SQLPBENGINE, MSSQLFDLauncher, SQLSERVERAGENT, MSSQLServerOLAPService, SSASTELEMETRY, SQLBrowser, SQLServerDistributedReplayClient, SQLServerDistributedReplayController, MsDtsServer150, SSISTELEMETRY150, SSISScaleOutMaster150, SSISScaleOutWorker150, MSSQLLaunchpad, SQLWriter, SQLTELEMETRY, MSSQLSERVER, BackExecRPCService, bedbg, Culserver, dbeng8, MSExchange, msftesql-Exchange, msmdsrv, MSSQL, sqladhlp, SQLADHLP, sqlagent, SQLAgent, SQLAgent$SHAREPOINT, tomcat6, vmware-converter, vmware-usbarbitator64, WSBExchange

표 5. 종료 대상 서비스

대상 서비스와 프로세스를 종료한 이후에는 암호화를 진행한다. -d 인자를 사용하면 특정 디렉터리와 그 하위 디렉터리만 암호화하며, -d 인자를 사용하지 않으면 CD/ROM 을 제외한 연결된 모든 드라이브를 암호화한다. 암호화 대상을 설정했으면, 각 디렉터리를 순회해 예외 항목에 해당하는지 확인하고 랜섬노트를 생성한다. 확인하는 암호화 예외 대상은 아래 표와 같다.

폴더명	확장자 및 파일명
AppData, Boot, C:\Windows, SYSVOL, Tor Browser, Internet Explorer, Google, Opera, Opera Software, Mozilla, Mozilla Firefox, $Recycle.Bin, ProgramData, All Users, bootmgr, system volume information, inte, msocache, perflogs, ntldr, Program Files, Program Files (x86), #recycle, $windows.~bt, ntuser.dat, NTUSER.DAT	HowToRecoveryFiles.txt, .exe, .dll, .sys, .drv, .bin, .tmp, .iso, .img, .direwolf

표 6. 암호화 예외 대상

파일 암호화는 파일의 크기에 따라 전체 암호화와 부분 암호화로 구분한다. 1MB 이하의 파일은 전체 데이터를 암호화하고, 1MB 보다 큰 파일은 파일의 첫 1MB 만 암호화한다. 각 암호화 대상 마다 랜덤한 개인키를 생성하고, 하드코딩된 DireWolf 의 공개키를 사용해 Curve25519 공유 비밀을 만들어 암호화에 활용한다. 해당 공유 비밀은 SHA-256 해시 알고리즘으로 해싱되어 암호화 키로 사용된다. 이 키는 다시 SHA-256 으로 해싱되며, 해당 해시의 일부를 nonce[1] 로 활용하여 ChaCha20 알고리즘으로 파일을 암호화한다. 파일의 끝에는 키 복구에 필요한 Curve25519 공개키와 함께 6 바이트 크기의 임의의 데이터(0xAB 0xBC 0xCD 0xDE 0xEF 0xF0)를 함께 저장한다.

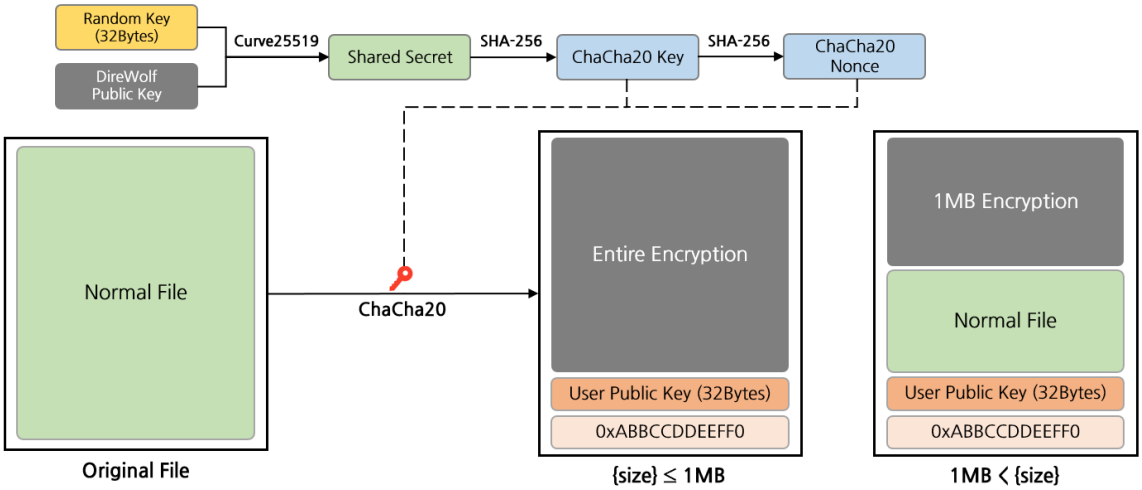


그림 12. 파일 암호화 방식

파일 암호화가 끝나면 C:\runfinish.exe 경로에 빈 파일을 생성하고 10 초 뒤 재부팅을 시도한다. 만약 재부팅에 실패하면 자가 삭제를 진행한 뒤 종료하고, 재부팅에 성공하면 자가 삭제는 진행되지 않는다. 사용하는 재부팅 명령어는 아래 표와 같다.

cmd /c start shutdown -r -f -t 10

표 7. 재부팅 명령어

[1] Nonce: 암호화에서 보안성과 고유성을 위해 사용되는 임의의 값

DireWolf 랜섬웨어 대응방안

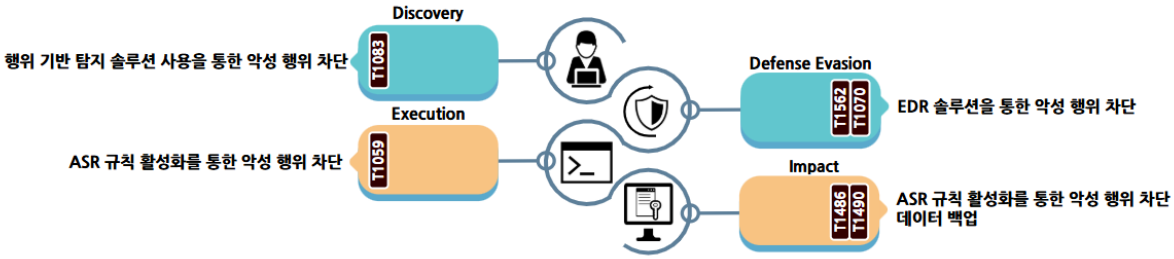


그림 13. DireWolf 랜섬웨어 대응방안

DireWolf 랜섬웨어는 중복 실행 방지를 위해서 실행 종료 시 runfinish.exe 라는 이름의 빈 파일을 생성하고, 실행 시에는 해당 파일이 시스템에 존재하는지 확인해 동일한 시스템을 중복으로 암호화하는 것을 방지하고 있다. 특정 경로의 파일을 검사하기 때문에 행위 기반 탐지 솔루션을 사용해 악성 행위를 탐지하고 차단할 수 있다.

악성 행위가 탐지되는 것을 회피하기 위해 이벤트 로그 프로세스를 중지하고 Windows 의 기본 이벤트 로그를 삭제한다. EDR[1] 솔루션을 사용해 특정 프로세스의 비활성화나 이벤트 로그 삭제와 같은 악성 행위를 차단할 수 있다. 또한, 분석 방지를 위해 자가 삭제 기능이 존재하는데, 이 역시도 EDR 솔루션을 사용해 악성 행위를 차단할 수 있다.

또한 앞서 설명한 DireWolf 랜섬웨어의 악성 행위는 Windows 명령 프롬프트를 활용해서 실행된다. 따라서 ASR[2] 규칙 활성화를 통해서 비정상적인 프로세스를 차단해 악성 행위를 막을 수 있다. 또한 암호화된 파일을 사용자가 임의로 복구하는 것을 방지하기 위해 총 9 개의 명령어를 활용해 시스템에 존재하는 모든 백업 복사본을 삭제하고, 복구 옵션을 비활성화한다. ASR 규칙 활성화로 파일 암호화는 물론 백업 복사본을 삭제하는 것을 차단할 수 있다. 또한, 백업 복사본을 별도의 네트워크나 저장소에 소산 백업하여, 시스템이 암호화되더라도 복구할 수 있도록 조치해야 한다.

[1] EDR (Endpoint Detection and Response): 컴퓨터와 모바일, 서버 등 단말기에서 발생하는 악성 행위를 실시간으로 감지하고 분석 및 대응하여 피해 확산을 막는 솔루션

[2] ASR (Attack Surface Reduction): 공격자가 사용하는 특정 프로세스와 실행 가능한 프로세스를 차단하는 보호 기능

IoCs

Hash(SHA-256)
8fdee53152ec985ffeeeda3d7a85852eb5c9902d2d480449421b4939b1904aad
27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3
b6fa7a34b57803d2b80f3f484656d34997231597b6c1aa7fc8a386d6474c8afe

■ 참고 사이트

• Group-IB (https://www.group-ib.com/blog/hunters-international-ransomware-group/)

• LE Parisien (https://www.leparisien.fr/high-tech/la-police-interpelle-cinq-hackers-francais-de-haut-vol-derriere-un-celebre-forum-de-vol-de-donnees-25-06-2025-QJTPFTDPQZAP7B25MF24YLHU6E.php)

• BleepingComputer (https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/)

Special Report

제로트러스트 보안전략 : 네트워크 (Network)

SI/솔루션사업그룹 보안 SI 사업팀 황병권 책임

■ 네트워크(Network) 필러 개요

네트워크는 모든 IT 인프라의 기반으로, 제로트러스트 환경에서 조직의 데이터·시스템·사용자·기기 등을 연결하는 핵심 매개체이다. 우리가 사용하는 이메일, 웹 서비스, 파일공유, 클라우드 업무, 원격접속 등 모든 디지털 활동은 네트워크를 매개로 이루어진다. 네트워크가 '모든 것을 연결한다'는 점은 곧 조직이 직면하는 대부분의 보안 위협이 네트워크를 통해 전파된다는 사실을 의미한다.

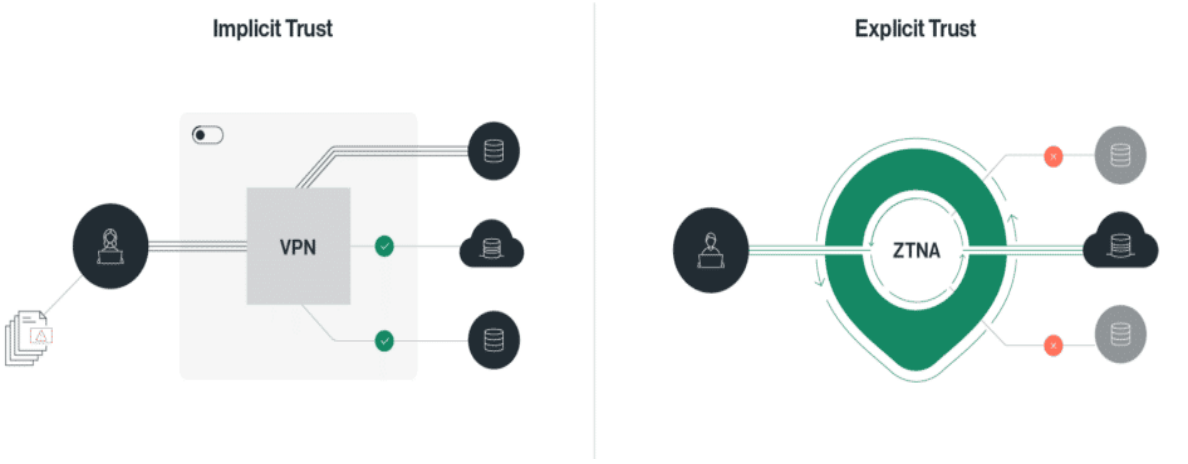
실제 침해사고·랜섬웨어·피싱·정보유출 등 오늘날 발생하는 대다수 공격은 네트워크 경유 없이 이뤄지는 경우가 거의 없다. 공격자는 네트워크 취약점, 비인가 접근, 내부 트래픽 위장, 암호화 우회, 세분화되지 않은 접근 정책 등 네트워크 상의 허점을 집요하게 파고든다. 최근에는 다크 웹 등지에서 네트워크 침투용 익스플로잇, VPN/프록시 계정, 망분리 우회 툴, 암호화 트래픽 해독 도구까지 실질적인 네트워크 공격 인프라 거래가 활발히 이루어지는 것이 현실이다.

기존 경계기반 보안 모델은 내부 네트워크를 신뢰 구역으로, 외부 네트워크를 비신뢰 구역으로 나누고 경계 방어에 집중하는 방식이었다. 하지만 클라우드 환경, 원격·재택근무의 증가 등 네트워크 환경이 급격히 다변화되면서, 이 전통적인 경계 보안 모델은 명확한 한계를 드러냈다. 경계 내로 침투한 위협을 탐지하거나 내부에서 확산되는 위협을 통제하는 데 어려움을 겪게 되었으며, 침해사고 발생 시 내부의 횡적 이동(Lateral Movement)을 효과적으로 방지하지 못하는 문제도 지속적으로 노출되었다.

특히 국내의 경우, 물리적 망분리를 중심으로 설계된 기존 보안 환경이 원격·유연 근무 확대에 따라 구조적 제약으로 작용하고 있으며, 이를 해소하기 위해 국가정보원 주도의 '국가 망 보안체계 가이드라인(N2SF)', 금융위원회의 '금융분야 망분리 개선 로드맵' 등에서 망분리 환경의 단계적 완화와 제로트러스트 기반 보완책을 함께 제시하고 있다. 제로트러스트 기반의 네트워크 아키텍처를 설계할 때 이러한 점도 충분히 고려하여 반영해야 한다.

이러한 문제를 해결하기 위한 대안으로 등장한 것이 ZTNA(Zero Trust Network Access, 제로트러스트 네트워크 접근제어)다. ZTNA 는 네트워크 접근을 요청하는 모든 사용자와 기기, 그리고 그 연결 행위를 기본적으로 신뢰하지 않고 항상 검증하는 원칙을 기반으로 한다. 내부·외부 네트워크 구분 없이, 모든 접근 요청은 실시간으로 사용자의 신원, 기기의 보안 상태, 접근 컨텍스트(위치, 시간, 행위 패턴 등)를 다각적으로 평가한 뒤, 검증된 사용자와 기기에 대해서만 최소 권한 원칙에 따라 리소스 접근을 허용한다.

ZTNA 접근 방식은 VPN 등 전통적인 경계기반 모델과 달리, 내부 네트워크 접근 시에도 사용자와 디바이스의 신뢰성을 지속적으로 평가하고 검증한다. 전통적인 경계 보안 방식은 네트워크에 한 번 접속하면 대부분의 내부 리소스에 광범위한 접근을 허용하는 '암묵적 신뢰(Implicit Trust)'를 기반한다. 반면, ZTNA 는 사용자·기기의 신뢰성을 매 순간 명시적으로 검증하는 '명시적 신뢰(Explicit Trust)' 방식을 적용한다. 이 접근 방식을 통해 조직은 네트워크 내부로 침투한 위협의 확산을 원천 차단하고, 세밀하고 동적인 접근 제어로 위협 대응 속도와 정확성을 크게 높일 수 있다.



출처 : Cato Networks, "Zero Trust Network Access (ZTNA)"

그림 1. 경계기반보안모델 vs ZTNA 모델

제로트러스트 아키텍처에서 네트워크 필러는 단순 연결 매개체를 넘어, 조직의 보안을 실질적으로 관리하고 위협을 지속적으로 탐지·차단하는 핵심적인 역할을 수행한다. 이러한 변화는 네트워크 환경의 복잡성 증가와 함께 진화하고 있으며, 조직은 이를 통해 더욱 강력하고 유연한 보안 환경을 구축할 수 있다.

■ 네트워크(Network) 필러의 주요 요소

모든 IT 자산과 서비스가 네트워크를 통해 상호 연결되는 구조적 특성상 네트워크 필러는 제로트러스트 아키텍처 환경에서 기술적 통제와 실제 보안 조치 시 가장 집중적으로 적용되어야 하는 핵심 필러다. 네트워크는 조직 내 데이터, 시스템, 사용자, 기기 등 모든 요소가 연결되는 기반이자, 실질적으로 보안 위협이 집중적으로 발생하는 주요 경로이기 때문에, 제로트러스트의 원칙을 실질적으로 구현하는 데 있어 가장 중요한 기술적 통제 영역으로 작동한다.

특히, 제로트러스트 환경에서는 네트워크 내부·외부를 구분하지 않고 모든 트래픽, 세션, 연결을 잠재적 위협으로 간주하며, 네트워크 흐름에 대한 실시간 가시성 확보와 동적·세분화된 정책 적용이 요구된다. 이를 위해 네트워크 인벤토리, 흐름 분석, 트래픽 암호화, 네트워크 접근제어, 논리적 경계 설정, 세그멘테이션, 네트워크 유연성 및 복원성, 가시성·모니터링 등 다양한 관리적·기술적 요소가 통합적으로 운영되어야 한다.

아래는 네트워크 필러의 주요 요소들과, 이를 구현하기 위한 구체적인 관리·기술 방안을 제로트러스트 성숙도 관점에서 정리한 내용이다.

1. 네트워크 인벤토리

제로트러스트 환경에서 네트워크 인벤토리는 조직 내 모든 유·무선 네트워크, 클라우드, 인터넷 접속을 포함한 다양한 통신 인프라와 이를 구성하는 물리적·논리적 네트워크 장비(스위치, 라우터, 무선 AP, 방화벽, SDN/SDP 장비 등)의 현황을 체계적으로 식별하고 관리하는 출발점이다. 관리 대상에는 전통적인 온프레미스 네트워크 장비뿐만 아니라, 클라우드 환경에 존재하는 가상 네트워크 장비, 원격지에 위치한 네트워크 장비까지 포함된다.

네트워크 인벤토리 관리의 핵심은 네트워크로 데이터를 송수신하는 모든 자산을 정확하게 식별하고, 장비의 도입·변경·이관·폐기 등 라이프사이클 전체에 걸쳐 정보가 최신 상태로 유지되는 것이다. 이를 위해 조직은 자산관리 시스템, 네트워크 모니터링 도구 등과 연계하여 네트워크 장비의 목록, 주요 속성(MAC, IP, OS, 하드웨어 사양 등), 사용 용도, 설치 위치, 소유 부서 등의 정보를 체계적으로 통합 관리해야 한다.

네트워크 장비는 그 용도와 역할(예: 업무망, 인터넷망, 클라우드망 등)에 따라 그룹화하여 관리할 수 있으며, 이러한 그룹 정보 역시 장비의 상태 변화(신규 도입, 용도 변경, 재배치 등)에 따라 자동으로 최신화되어야 한다. 그룹별로 정책을 차등 적용하거나, 네트워크 세그멘테이션, 접근제어 등과 연계해 활용할 수 있다.

네트워크 인벤토리는 단순한 목록 관리에 그치지 않고, 네트워크 망의 논리적·물리적 구조까지 아우른다. 업무망, 인터넷망, 클라우드망 등 조직 내 다양한 네트워크 영역(망)은 각각 명확하게 정의되어야 하며, 망별로 포함된 장비·연결 구조·트래픽 흐름·보안 정책 등이 체계적으로 관리되어야 한다. 이러한 망 정의는 SDN/SDP, 네트워크 세그멘테이션 등 차세대 네트워크 아키텍처 적용 시 기술적 기준이 된다.

성숙도가 높은 조직의 경우, 모든 네트워크 리소스는 도입 시 자산관리 시스템에 자동 등록되고, 네트워크 변화가 발생할 때마다 통합 모니터링 시스템과 연동하여 실시간으로 토폴로지 정보가 제공된다. 또한, 네트워크 장비의 상태 및 변경사항에 대한 가시성이 확보된다. 이로써 조직은 네트워크 인벤토리 기반으로 네트워크 접근제어, 이상 행위 탐지, 장애 대응 등 다양한 네트워크 보안 및 운영정책을 효과적으로 적용할 수 있다.

2. 네트워크 흐름 분석

제로트러스트 환경에서 네트워크 흐름 분석은 조직 내 네트워크를 통해 오가는 모든 트래픽과 연결 정보를 실시간으로 모니터링하고, 트래픽 패턴 및 이상 행위를 탐지·분석하는 핵심적인 보안 활동이다. 이는 네트워크를 통한 위협이나 비인가 접근을 조기에 식별하고, 신속하게 대응하기 위한 필수 절차로 자리잡고 있다.

네트워크 흐름을 분석하기 위한 출발점은 네트워크 전체의 트래픽 경로, 주요 연결 포인트, 내부·외부간 통신 흐름을 정확하게 파악하고, 업무망, 인터넷망, 클라우드망 등 네트워크 영역별 트래픽의 정상 기준선을 수립하는 것이다. 조직은 네트워크 모니터링 시스템, 트래픽 분석 도구 등을 활용해 패킷 흐름, 연결 현황, 데이터 전송량, 주요 통신 대상 등을 체계적으로 수집·분석해야 한다.

이 과정에서 네트워크 라우팅 및 아키텍처에 대한 주기적 현행화와 시각화가 병행되어야 하며, 네트워크 세그멘테이션, SDN/SDP 등 논리적 경계의 도입 여부와 연동되어 네트워크 전체 구조와 흐름을 통합적으로 관리할 수 있어야 한다. 네트워크 라우팅 및 아키텍처 정보는 정책 기반 네트워크 접근제어, 이상 트래픽 탐지, 장애 대응 등 다양한 네트워크 보안 운영의 기초 데이터로 활용된다.

네트워크 흐름 분석을 통한 통합 모니터링 시스템과 연계한 실시간 네트워크 흐름 가시성 확보는 제로트러스트 환경의 핵심 요구사항이다. 성숙도가 높은 조직은 네트워크 연결 변화, 흐름 이상, 라우팅 구조 변경 등 네트워크 전반의 변동사항을 자동으로 감지하고, 분석 결과를 기반으로 네트워크 보안 정책에 신속하게 반영할 수 있다.

3. 네트워크 트래픽 암호화

제로트러스트 환경에서 네트워크 트래픽 암호화는 내부·외부 구분 없이 모든 네트워크 구간의 데이터 전송 과정에서 기밀성과 무결성을 보장하기 위한 필수 요소다. 네트워크를 통해 오가는 대부분의 트래픽은 TCP, UDP 와 같은 전통적 프로토콜을 기반으로 해 TLS, DTLS 등 표준 암호화 프로토콜을 적용해 트래픽 자체를 암호화한다. 이로써 데이터는 중간자 공격, 패킷 탈취, 트래픽 변조 등 다양한 위협으로부터 보호된다. 특히, 중요도가 높은 구간이나 민감 정보가 오가는 트래픽은 암호화 정책에 따라 반드시 보호되어야 하며, 암호화 프로토콜 자체의 취약점이 발견될 경우 즉각적인 패치 및 대응 체계를 마련해야 한다.

DNS 트래픽 또한 암호화가 반드시 요구되는 영역이다. DNS 의 설계는 원래 보안을 염두에 두지 않았기 때문에 스푸핑, DOS, 중간자 공격 등 다양한 취약점에 노출될 수 있다. 이에 따라 DNSSEC 와 같은 디지털 서명 기반의 프로토콜, HTTPS/TLS 기반의 DOH(DNS over HTTPS), DOT(DNS over TLS) 등 암호화 기술이 적용되고 있으며, 암호화로 인한 성능 저하, 관리 복잡성, 호환성 문제에 대해서도 사전에 대응 방안을 마련해야 한다. 특히, DOT 프로토콜이 성능 및 관리 효율성 측면에서 권장되며, DNS 트래픽에 대한 전 방위적 암호화 적용이 점차 확대되는 추세다.

제로트러스트 환경에서는 TCP/UDP 외에도 ICMP, SCTP 등 기타 네트워크 트래픽도 암호화가 필요하다. ICMP 와 같이 자체 암호화가 어려운 프로토콜은 IPSEC 등 별도의 보안 기술을 적용할 수 있고, SCTP 는 DTLS 와 같은 암호화 기술을 활용한다. 또한 SSL VPN 터널링, 트래픽 캡슐화 등 다양한 방식으로 네트워크 내외부의 모든 트래픽이 안전하게 보호되도록 설계해야 하며, 이러한 암호화 정책과 실행 상태는 모니터링 및 로그 분석 시스템과 연동해 실시간으로 가시성을 확보해야 한다.

최근에는 전통적인 암호화 방식의 한계를 극복하기 위해, 양자암호화(Quantum Cryptography) 기술을 VPN 터널링 등 네트워크 암호화 채널 위에 적용하려는 시도가 이어지고 있다. 양자암호키분배(QKD, Quantum Key Distribution) 기술을 활용해 기존 VPN 통신에 양자 난수 기반의 암호키를 적용함으로써, 이론적으로는 중간자 공격이나 미래의 양자컴퓨팅 기반 해킹에도 방어할 수 있는 보안성을 기대할 수 있다. 다만, 현재 이러한 양자암호화 기반 네트워크 암호화 기술은 일부 실증적 프로젝트와 시범 사업 단계에 머물러 있으며, 실제 조직 환경에서 상용화 및 현행 업무에 본격적으로 적용되는 사례는 아직 드문 상황이다.

4. 네트워크 액세스 관리

제로트러스트 환경에서 네트워크 액세스 관리는 조직 내 모든 네트워크 리소스에 대한 접근을 정밀하게 통제하고, 실시간으로 인증·인가·모니터링함으로써 내부·외부 위협에 대한 보안 수준을 극대화하는 핵심 영역이다. 네트워크 액세스 관리는 네트워크 접근제어, 인증, 인가, 그리고 인증 연동 등으로 구성되며, 각 단계는 상호 연계되어 조직 전체 네트워크의 신뢰성과 가시성을 높인다.

네트워크 접근제어는 방화벽, NAC, IPS 등 다양한 보안 장비로 네트워크 리소스 접근 정책을 세분화하고, 네트워크 내 세션·트래픽을 실시간으로 제어한다. 최근에는 SDP(Software Defined Perimeter), Micro Segmentation 등의 기술을 활용하여 네트워크 접근 경로를 논리적으로 세분화하고, 사용자나 디바이스의 신뢰도, 위치, 행위 정보 등을 기반으로 세분화된 접근 정책을 동적으로 적용한다. ICAM 등과 연동할 경우, BYOD 나 외부 디바이스, 위험도가 높은 네트워크 엑세스 세션까지도 통합적으로 모니터링·차단할 수 있다.

네트워크 액세스 인증은 단순히 장비 기반의 인증에 머무르지 않고, AD, LDAP, IAM 등 계정 관리 시스템 및 SSO, MFA 와 연동하여 네트워크 리소스 접근 시 사용자의 신원과 디바이스 정보를 함께 검증한다. SDP, Micro Segmentation 구간에서는 더욱 엄격한 인증·인가 정책이 적용되며, 인증 정보뿐만 아니라 실시간 행위 분석, 리스크 기반 인증, 추가 인증 등도 병행된다.

네트워크 액세스 인가는 인증된 사용자·디바이스가 실제로 어떤 네트워크 리소스에 언제, 어디서, 어떤 권한으로 접근할 수 있는지 세분화해 관리하는 절차다. 인가 정책에는 시간, 위치, 사용자의 역할, 접속 이력 등 다양한 컨텍스트 정보가 반영되며, ICAM, 통합 모니터링 시스템 등과 연동하여 네트워크 인가 세션을 지속적으로 점검하고, 이상 징후 발생 시 세션 종료 또는 재 인증이 자동으로 이뤄질 수 있도록 한다. 취약점 관리 결과는 디바이스 위험도 평가에 직접 반영할 수 있다. 반복적으로 취약점이 발견되거나, 미조치 상태가 지속되는 기기는 민감 데이터 접근 제한, 추가 인증 요구, 네트워크 분리 등으로 연동해 실질적 리스크를 줄일 수 있다.

네트워크 액세스 인증 연동은 조직 내 모든 네트워크 환경(유선, 무선, RADIUS 등)에서 통합 계정관리 및 인증 시스템과 연계하여 네트워크 접근 과정 전체를 일관되게 관리한다. 인증·인가를 세션 단위로 실시간 처리하고, 다양한 인증 시스템 간 표준 프로토콜(API, SAML, RADIUS, TACACS+ 등)과 연동하여 인증 효율성과 보안성을 극대화할 수 있다. 네트워크 액세스 관리는 전통적인 경계 기반 통제에서 한 단계 더 진화해, 세분화된 인증·인가·모니터링 체계를 통합적으로 운영함으로써, 네트워크 내외부의 다양한 위협에 선제적으로 대응하고, 조직 전체의 보안 신뢰성을 높이는 핵심 기반이 된다.

5. 소프트웨어 정의 경계(SDN/SDP)

제로트러스트 환경에서 소프트웨어 정의 경계(SDN/SDP)는 네트워크를 가상화하고 논리적 경계를 동적으로 설정함으로써, 네트워크 공격 표면을 획기적으로 줄이고 중요 데이터 및 서비스에 대한 접근을 세밀하게 통제할 수 있도록 지원하는 핵심 기술 영역이다. SDN(Software Defined Networking)과 SDP(Software Defined Perimeter)는 기존의 물리적 경계 기반 네트워크 보안을 논리적으로 재정의한다. 정책 기반 라우팅, 네트워크 세그멘테이션, 동적 엑세스 제어 등의 기술로 네트워크를 다수의 논리적 영역으로 분리하는 것이다.

SDN/SDP 기반 논리적 경계 설정은 네트워크 및 시스템 구성도를 토대로, 네트워크 내 여러 개의 논리적 영역(Zone)을 정의하고, 각 영역별로 접근 정책과 인증·인가 기준을 차별화하는 것이 핵심이다. 논리적 경계별로 별도의 게이트웨이 및 인증 시스템과 연계하여, 각 영역에 대해 식별자·디바이스·애플리케이션의 신뢰도를 다층적으로 검증한 뒤 접근을 허용한다. 나아가 통합 모니터링 시스템과 연동하여 논리적으로 분리된 네트워크 영역에 대한 실시간 가시성 확보와 경계별 동적 정책 적용이 가능하다.

특히 SDN/SDP 환경에서 사용자 ID 확인은 모든 리소스 접근의 출발점이 된다. SDN/SDP 자체 인증 외에도 IAM, ICAM 등 계정 및 신원 관리 시스템과의 연동을 통해, 접근 사용자의 신원·행위·위험도 등을 다각적으로 검증한다. 초기 접근 시에는 사용자 ID 및 자격 증명을 필수적으로 확인하며, MFA, Passwordless 인증 등 다양한 인증 방식을 환경에 맞게 선택적으로 적용할 수 있다. 또한 SPA(Single Packet Authorization) 등 선 인증 기술을 활용해, 신뢰 정보가 포함된 싱글 패킷 기반의 인증과 지속적 인증 검증으로 사용자 세션 전체에 대한 보안성을 높일 수 있다. SDN/SDP 기반의 소프트웨어 정의 경계는 기존 네트워크의 경계 한계를 극복하고, 실시간 가시성과 동적 통제, 세분화된 인증·인가 정책을 결합하여 조직 네트워크의 보안 신뢰성을 한 차원 더 강화하는 역할을 수행한다.

6. 네트워크 분할(Segmentation)

제로트러스트 환경에서 네트워크 분할은 공격 표면을 최소화하고, 네트워크 내부에서 발생할 수 있는 위협의 확산을 효과적으로 차단하기 위한 핵심 통제 수단이다. 기존의 네트워크는 하나의 넓은 평면(topology) 상에서 많은 시스템과 서비스가 자유롭게 통신하는 구조였으나, 제로트러스트 아키텍처에서는 네트워크를 논리적으로 다수의 구역(zone)으로 분할하고, 각 구역마다 세분화된 보안 정책과 통제 기준을 적용해 Lateral Movement(횡적 이동)을 방지한다.

매크로 세그멘테이션(Macro Segmentation)은 네트워크를 서브넷, VLAN, 또는 시스템 그룹 등으로 분할해 트래픽 흐름을 제어하고, 기능·부서·위치 등 고수준 기준에 따라 네트워크 영역을 구분한다. 이를 통해 부서 간 또는 중요 시스템과 일반 사용자 구간을 명확히 분리해, 네트워크 트래픽을 효과적으로 통제하고, 내부 위협이나 공격이 전체 네트워크로 확산되는 것을 방지한다. 방화벽, VLAN 등 전통적 네트워크 분할 기술을 활용하여 논리적으로 인프라와 시스템을 그룹별로 관리하며, 실시간 모니터링 시스템과 연계해 변화에 신속하게 대응할 수 있다. Macro Segmentation 이 자동화된 환경에서는 정책에 따라 네트워크 그룹의 추가·변경·분할이 자동으로 반영된다.
마이크로 세그멘테이션(Micro Segmentation)은 매크로 세그멘테이션 보다 세밀한 수준에서 네트워크 구간을 분리한다. 기존의 서브넷·VLAN 과 같은 경계가 아닌, 애플리케이션, 사용자, 작업량, 데이터 유형 등의 다양한 기준으로 네트워크 내 자산 및 트래픽을 세분화하는 것이다. 각 그룹 또는 라벨(Label) 단위로 맞춤화된 접근 정책과 통제 기준을 동적으로 적용하며, 인벤토리, 인증, 자산 관리 시스템과 연동해, 중요 자산이나 구역에 특화된 보호 대책을 구현한다. 마이크로 세그멘테이션은 네트워크 내 보안 위협을 조기에 탐지하고, 이상 트래픽이나 의심스러운 활동이 발생할 경우 자동화된 방식으로 정책을 변경하거나 차단할 수 있도록 지원한다. 전사적 적용 시, 시스템 및 데이터 변화에도 실시간으로 세분화 정책이 반영되어 유연한 보안 대응이 가능하다.

제로트러스트 환경에서 네트워크 분할 전략은 단순한 물리적 경계를 넘어서, 조직의 다양한 업무 환경과 자산 특성에 맞는 세분화된 접근 통제와 자동화된 정책 운영을 결합하여, 네트워크 내 리스크를 최소화하고, 실질적인 내부 확산 방지와 유연한 보안 환경을 동시에 실현할 수 있게 한다.

7. 네트워크 유연성

제로트러스트 환경에서 네트워크 유연성은 예측 불가능한 장애, 성능 저하, 다양한 위협에도 불구하고 비즈니스 연속성과 서비스 가용성을 보장하기 위한 핵심 관리·운영 요소다.

네트워크 유연성은 가용성, 복원성, 백업 관리의 세 가지 핵심 축을 중심으로 구축된다.

먼저, 네트워크 가용성 확보는 평상시뿐만 아니라 장애 발생 시에도 네트워크의 정상 동작을 보장하는 것이 목표다. 조직은 네트워크 장애 예방, 신속한 장애 감지 및 복구, 실시간 성능 모니터링, 예방적 유지보수 체계, 실시간 알림 및 보고 등 다양한 관리 체계를 갖춰야 한다. 이를 통해 네트워크 중단 시간을 최소화하고, 업무 및 서비스 연속성을 항상 유지할 수 있도록 한다.

네트워크 복원성은 장애 발생 시 수동 혹은 자동화된 절차로 네트워크 구성 요소, 설정, 데이터를 신속하게 복구해 네트워크 서비스 중단 시간을 최소화하는 것을 의미한다. 주요 구간 이중화, 주기적인 Fail Over 테스트 등 사전 준비를 바탕으로, 실제 장애가 발생 시 네트워크 백업 시스템과 연동된 복구 정책에 따라 자동 복원이 이루어진다. 특히 SDN/SDP 등 차세대 네트워크 기술과 연계해, 모니터링 및 대응 시스템이 자체적으로 이상 상황을 진단하고 자동 복구를 실행할 수 있도록 하는 것이 이상적인 목표다.

마지막으로, 네트워크 백업 관리는 네트워크 구성 요소, 설정, 데이터 등을 수동 또는 자동으로 정기 백업하여, 장애·오류 등 비상 상황에서도 백업 데이터를 기반으로 신속히 복원할 수 있게 하는 체계를 의미한다. 조직은 다양한 백업 유형과 저장소를 활용해 백업 데이터의 안정성과 가용성을 높이고, 암호화 및 압축 등 보안 기능을 적용해 백업 데이터 유출이나 변조 위험도 예방해야 한다.

네트워크 유연성은 제로트러스트 환경에서 예측하지 못한 다양한 리스크에 대응하고, 비즈니스 연속성을 유지하기 위한 구조적 기반을 제공한다.

8. 네트워크 모니터링 및 분석

제로트러스트 환경에서 네트워크 모니터링 및 분석은 네트워크의 상태, 트래픽 흐름, 이상 징후 등을 실시간으로 감지·분석하여, 위협을 조기 탐지하고 대응하는 핵심 관리 체계다. 네트워크가 복잡·확장될수록 전체 인프라의 '가시성' 확보가 필수적이며, 모니터링·분석 체계의 정교함에 따라 보안 위협 대응 역량도 크게 좌우된다.

네트워크 가시성 확보는 실시간 모니터링을 통해 네트워크의 상태와 구성, 장비 변화, 네트워크 토폴로지 등을 명확히 파악하는 것을 의미한다. 조직은 네트워크 인벤토리 및 주요 네트워크 구간을 기준으로 가시화 정책을 수립하고, 변화가 발생할 때마다 자동으로 가시성이 확보될 수 있는 자산관리·모니터링 시스템을 연동해 운영해야 한다. 이를 통해 네트워크 내 장비·구역별 실시간 변화, 연결 상태, 잠재적 보안위험 요소까지 빠짐없이 파악할 수 있다.

네트워크 모니터링은 트래픽 흐름, 성능 지표, 접속 이력, 이상 트래픽 등을 실시간으로 점검하며, 탐지·대응 시스템과 연계하여 자동화된 대응체계를 함께 구축하는 것이 중요하다. 제로트러스트 환경에서는 TCP/IP 트래픽 위주의 전통적인 네트워크 모니터링을 넘어서, DNS, ICMP, SCTP 등 다양한 트래픽 유형에 대한 실시간 모니터링과 분석 체계도 반드시 갖추어야 한다. DNS 트래픽의 경우, 스푸핑, 비정상 쿼리, 캐시 오염 등 특유의 취약점이 존재하므로, DNS 트래픽의 사용량과 패턴, 이상 징후를 실시간으로 분석하고, 필요시 자동화된 정책을 통해 DNS 서버 설정 변경이나 캐시 초기화 등의 대응이 이루어져야 한다. 마찬가지로, ICMP, SCTP 등 기타 네트워크 트래픽 역시 잠재적 위협 탐지와 네트워크 상태 진단을 위해 주기적이고 자동화된 분석이 필요하다.

네트워크 트래픽 분석은 조직 내 모든 트래픽을 수집·분석·시각화하여, 트래픽 패턴, 이상 행위, 잠재적 공격 신호 등을 종합적으로 분석하는 작업이다. 실시간 분석 데이터를 바탕으로 모니터링 시스템·탐지 시스템 등과 연계하여, 보안 위협에 대한 자동 대응과 네트워크 성능 최적화까지 실질적으로 구현한다. 이상 트래픽 발생 시 다양한 보안 시스템과 연계해 즉각적으로 탐지·분석·대응이 가능한 구조를 갖추는 것이 중요하다.

결국 네트워크 모니터링 및 분석 체계의 고도화는 조직 네트워크 전체의 투명성과 실시간 대응 역량을 높이고, 제로트러스트 환경에서 요구되는 '지속적 검증'과 '자동화 대응'의 실질적 기반을 제공한다. 이상 트래픽 발생 시 다양한 보안 시스템과 연계해 즉각적으로 탐지·분석·대응이 가능한 구조를 갖춰야 한다.

9. 네트워크 리소스 관리

제로트러스트 환경에서 네트워크 리소스 수명주기 관리는 모든 네트워크 구성 요소(스위치, 라우터, 방화벽, 가상 네트워크 등)에 대해 도입, 운영, 변경, 폐기에 이르는 전 생애주기 전체를 체계적으로 관리하는 것을 의미한다.

조직은 네트워크 리소스의 프로비저닝(자동 배포), 실시간 모니터링, 정책 기반 자동 대응, 리포팅 및 분석 등 다양한 기능을 통합하여, 각 리소스의 상태 변화와 사용 이력, 운영 정책 준수 여부, 위험 요인 등을 한눈에 파악하고 관리할 수 있도록 해야 한다.

특히, 네트워크 환경의 변화에 따라 장비의 도입, 구성 변경, 사용 중지, 폐기 등 다양한 이벤트가 발생할 수 있으므로, 모든 리소스가 정책과 원격 측정(telemetry) 기반으로 정의된 수명을 갖도록 관리하는 것이 중요하다.

자동화된 변경 관리 시스템, 모니터링 도구와의 연계를 통해 네트워크 환경 및 리소스의 수명 주기를 실시간으로 관리할 수 있으며, 예기치 못한 장애나 보안 위협 발생 시 신속하게 자동 대응할 수 있는 체계도 갖추어야 한다.

성숙도가 높은 기관의 경우, 네트워크 리소스의 생성과 종료(시작·만료), 변경 이벤트가 코드형 인프라(IaC: Infrastructure as Code) 기반으로 자동화되어 관리되며, 전체 리소스의 수명 주기에 걸쳐 운영 효율성과 안정성, 보안성을 동시에 강화할 수 있다. 정책과 프로세스의 정교화는 디바이스 및 엔드포인트 영역의 일관된 보안 태세 유지와, 변화하는 업무 환경에서의 신속한 위험 대응에 반드시 필요한 기반이다.

10. 네트워크 정책 및 프로세스

제로트러스트 아키텍처에서 네트워크 보안 정책 및 프로세스는 조직의 보안 수준을 일관성 있게 유지하고, 변화하는 위협에 신속하게 대응하기 위한 핵심 기반이다. 네트워크 운영과 시스템 운영은 분리되어 운영되어야 하며, 필요한 서비스에서만 사용자가 접근할 수 있도록 최소 권한 원칙을 적용한 보안 정책 수립이 필수적이다. 네트워크 운영 및 유지관리, 변경 요청, 장비 및 구성 관리, 원격지 장비 관리 등 모든 세부 프로세스는 명확한 지침과 책임자 지정, 위험 분석 및 대응 방안, 정책 변경 이력 관리 등을 포함해야 한다.

네트워크 접근 정책은 비인가 접근 통제(IP 관리, 단말 인증 등), 서비스 및 포트 차단, 인증 프로세스 등 다양한 관점에서 정의되며, 중요도와 업무 목적에 따라 실시간 모니터링 및 이상 접근 탐지, 자동화된 접근 제한 등으로 고도화되어야 한다. 네트워크 아키텍처 관리 역시 주기적인 검토와 구조 현행화, 토폴로지 맵 및 장비 연동 상태의 자동화된 관리가 필요하다.

원격지 네트워크 장비 관리의 경우, 보호구역 외부에서의 정보 시스템 운영은 원칙적으로 제한하되, 불가피한 경우 책임자 승인, 접근 단말 지정, 허용 범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속 단말 보안(백신, 패치 등)과 같은 다양한 보호대책을 수립·이행해야 한다.

최근에는 온프레미스 환경뿐만 아니라 다양한 멀티 클라우드, 하이브리드 네트워크 환경이 조직 내 표준이 되고 있다. 이에 따라 기존 정책 및 프로세스 역시 클라우드 네이티브 인프라와 연계할 수 있도록 확장·재정립되어야 하며, 정책 적용의 자동화, 환경 변화에 따른 정책 유연성, 그리고 통합 모니터링 및 감사체계 구축 등도 함께 고려해야 한다.

위와 같은 주요 요소들을 기반으로, 네트워크 필러는 제로트러스트 아키텍처 내에서, 모든 IT 자산과 서비스가 네트워크를 통해 상호 연결되는 조직의 구조적 특성상 데이터, 시스템, 사용자, 기기 등 전체 보안과 신뢰성을 결정짓는 가장 중요한 경로이자, 보안 위협이 집중되는 핵심 지점이다.

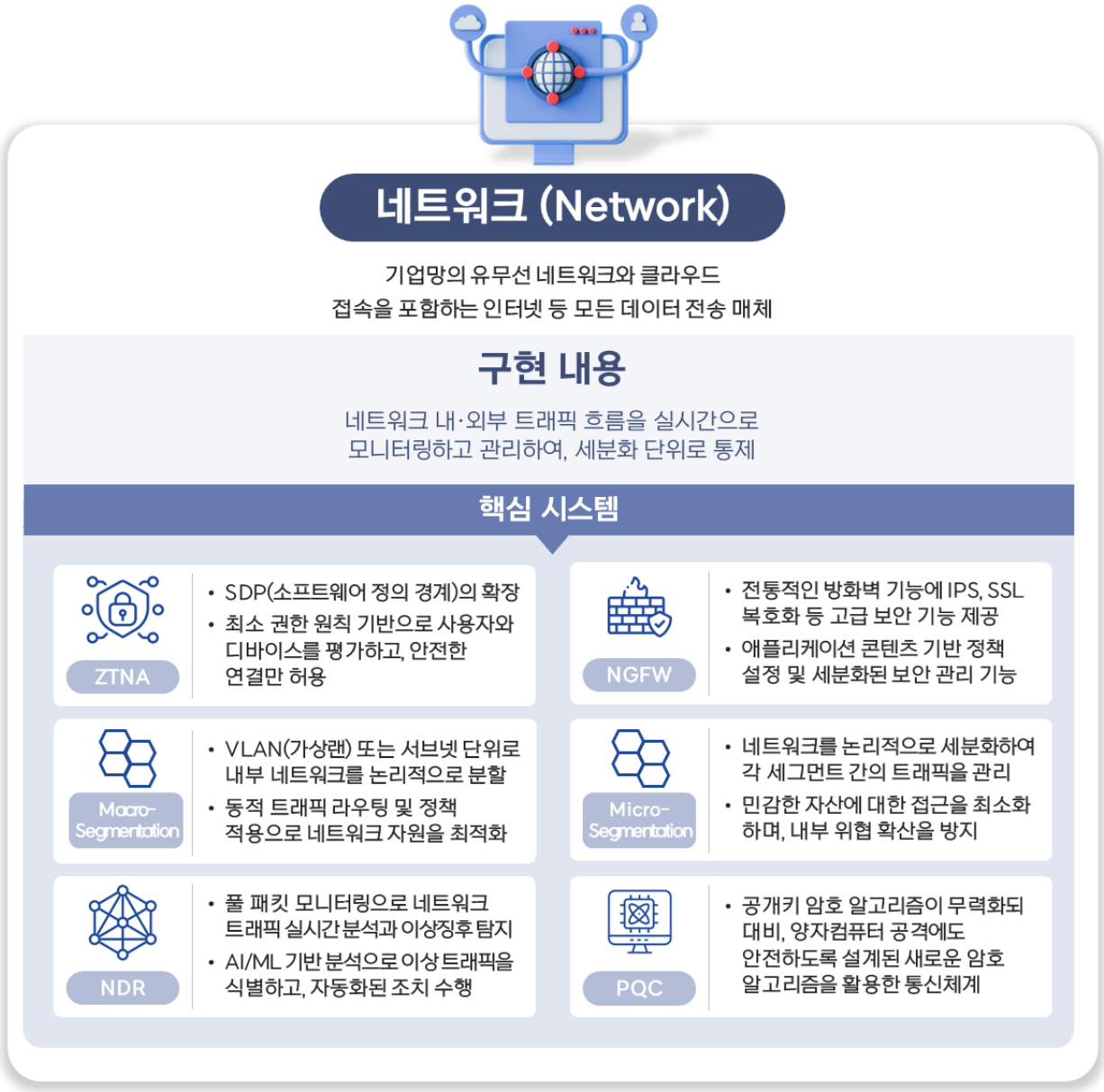
특히, 제로트러스트 환경에서는 네트워크 내부·외부 구분 없이 모든 트래픽과 연결을 잠재적 위협으로 간주하고, 실시간 가시성 확보, 동적·세분화된 정책 적용, 트래픽 암호화, 세그멘테이션, 액세스 제어, 논리적 경계 및 복원성 확보 등 다양한 관리적·기술적 요소가 유기적으로 연계되어야 한다.

이를 통해 조직은 네트워크 흐름 전반에 걸쳐 위협을 조기에 탐지하고, 자동화된 통제 및 대응이 가능한 구조를 실현할 수 있다. 네트워크 필러의 고도화는 제로트러스트 원칙이 조직 전체 인프라에 일관되게 적용되는 실질적 기반이 되며, 급변하는 IT 환경과 진화하는 보안 위협에 신속하고 유연하게 대응할 수 있는 디지털 보안 체계를 완성하는 핵심 동력으로 작용한다.

■ 주요 시스템별 제로트러스트 기능 구현

제로트러스트 환경을 성공적으로 구현하기 위해서는 기술적 방안과 이를 수행할 수 있는 시스템은 필수적이다. 제로트러스트 아키텍처는 "신뢰하지 않고 항상 검증한다"는 원칙 하에, 이를 실현하기 위해 네트워크 상태를 확인하고, 지속적으로 검증하며, 최소 권한 접근을 보장을 수행해야 한다.

아래 주요 시스템 등은 각각 제로트러스트 환경에서 중요한 역할을 담당하며, 이들 시스템은 상호 연계되어 조직의 보안 태세를 강화할 수 있다. 각 시스템 별로 제로트러스트 환경 구현을 위해 수행해야 할 기능과 이를 통해 조직이 얻을 수 있는 보안 강화 효과를 구체적으로 살펴보고자 한다.



출처 : SK 쉴더스, "제로트러스트의 시작:SKZT 로 완성하다"

그림 2. 네트워크 주요 시스템

1. ZTNA (Zero Trust Network Access, 제로트러스트 접근제어)

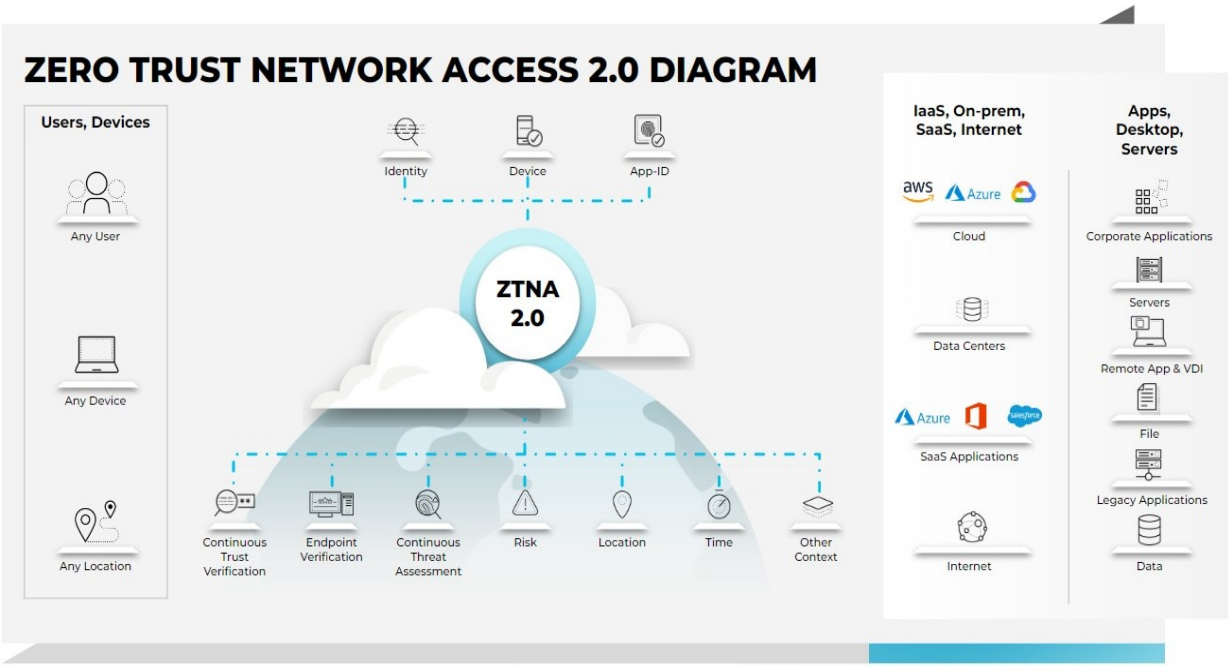
ZTNA 는 제로트러스트 아키텍처의 핵심 원칙인 “신뢰하지 않고, 항상 검증한다”는 접근 통제 모델을 네트워크 영역에 적용한 대표적 기술로, 기존의 신뢰 기반(Perimeter-based) 네트워크 접근 모델과 근본적으로 다르다.

ZTNA 환경에서는 모든 네트워크 접근 요청을 신뢰하지 않는다. 사용자의 신원, 디바이스 상태, 위치, 시간, 행위 패턴 등 다양한 컨텍스트 정보를 실시간으로 검증한 뒤, 인가된 트래픽에 한해서만 내부 네트워크와 리소스에 접근을 허용한다. 이 과정에서 네트워크 내부(온프레미스, 사내)와 외부(원격, 클라우드 등) 모두에 대해 동일하게 적용되는 일관된 접근 통제 체계를 제공한다.

초기 ZTNA 는 SDP(Software-Defined Perimeter) 기반으로 등장했으나, 현재는 다양한 네트워크 접근 기술(차세대 방화벽, NAC, VPN/SSL-VPN 등)과 결합하여 각 벤더별·솔루션별로 고유의 방식으로 구현되고 있다. 실제 시장에서 ZTNA 는 ‘아키텍처적 개념’뿐 아니라, 각 벤더의 제품(솔루션)으로도 구분·제공되고 있으며, 도입 형태와 태생에 따라 지원하는 기능과 세부 구현에 상당한 차이가 존재한다.

예를 들어, 차세대 방화벽(NGFW) 기반 ZTNA 는 사용자의 신원과 디바이스 상태를 식별하고, 애플리케이션 인지 및 세분화된 정책 기반 접근통제, 마이크로 세그멘테이션로 인가된 사용자나 기기만 특정 네트워크 세그먼트에 접근할 수 있도록 엄격히 통제한다. 반면, NAC(Network Access Control) 기반 ZTNA 는 주로 사내 LAN 등 내부 네트워크 환경에 최적화되어, 엔드포인트의 상태와 인증 정보, 패치·백신 등 보안 점검 결과를 실시간으로 평가하여 네트워크 접근을 허용·차단하는 구조로 운영된다. 또한, VPN 또는 SSL-VPN 기반 ZTNA 는 기존 원격접속 방식에 사용자·기기 검증, MFA, 위치·행위 분석 등 추가적인 검증 요소를 결합함으로써, 원격 환경에서도 세분화된 접근 통제와 안전성을 동시에 확보하는 방식으로 진화하고 있다.

ZTNA 시스템은 대체로 정책 결정 지점(PDP, Policy Decision Point)과 정책 시행 지점(PEP, Policy Enforcement Point)으로 구성된다. PDP 는 네트워크 접근 요청이 들어올 때마다 사용자의 신원, 기기 상태, 위치, 행위 패턴 등 다양한 컨텍스트 정보를 다각적으로 평가해 접근 허용 여부와 범위를 동적으로 결정하며, 인가된 요청에 한해 PEP 가 실제 네트워크 또는 리소스에 대한 접근을 중개하고 통제한다. 이처럼 ZTNA 는 온프레미스, 클라우드, 하이브리드 등 다양한 환경에서 유연하게 구축될 수 있으며, 최근에는 SASE(Secure Access Service Edge) 등 클라우드 기반 플랫폼과 결합되어 원격근무, 멀티클라우드 등 분산된 인프라 환경에서도 일관된 제로트러스트 접근통제를 실현하고 있다.



출처 : Paloalto, "What is Zero Trust Network Access"

그림 3. Paloalto ZTNA 2.0 DIAGRAM

ZTNA 는 네트워크 내·외부 구분 없이 모든 트래픽, 세션, 연결을 잠재적 위협으로 간주하고, 실시간 가시성 확보와 동적 정책 적용, 미인가/취약 사용자·디바이스의 접근 원천 차단, 세그멘테이션 기반의 횡적 이동(Lateral Movement) 방지 등 현대 네트워크 환경에서 요구되는 실질적 보안 요구를 구현한다. 이러한 시스템은 각 벤더의 기술적 기반(방화벽, NAC, VPN 등)에 따라 네트워크 환경(내부/외부/클라우드)별 최적화 수준, 정책 세분화, 인증 연동, 사용자 경험, 운영 효율성 등에서 구현 방식의 차별성이 크기 때문에, 실제 도입 시에는 조직의 환경과 업무 특성을 충분히 고려해 설계·선정하는 것이 매우 중요하다.

2. NGFW (Next-Generation Firewall, 차세대 방화벽)

NGFW 는 단순한 IP·포트 기반의 전통적 경계 방어에서 진화해, 네트워크 트래픽을 애플리케이션 레벨까지 식별하고 정밀하게 제어하는 네트워크 보안 시스템이다. 네트워크 계층(L3, L4)에서의 제한적 트래픽 통제만으로는 업무 목적에 따라 다양한 애플리케이션의 사용과 보안 요구를 충족하기 어렵다. NGFW 는 업무에 필요한 클라우드 서비스, Microsoft 365(M365)와 같은 SaaS, 특정 SNS 등 비즈니스 목적에 맞는 애플리케이션은 허용하고, 불필요하거나 위험성이 높은 서비스는 선택적으로 차단하는 세분화된 정책을 제공한다.

SD-WAN(Software-Defined Wide Area Network)과 VPN/SSL-VPN 등 연계 기능을 통합 지원하여, 본사·지점·원격근무 등 분산된 조직 환경에서도 안전한 네트워크 연결과 정책 적용을 동시에 실현시킨다. 사용자, 기기, 애플리케이션 속성에 따라 논리적 네트워크 세그먼트를 정의하고, 각 세그먼트별로 서로 다른 접근 정책을 적용함으로써, 내부 침해 발생 시 피해 확산을 효과적으로 차단할 수 있다. 네트워크 트래픽의 흐름을 세밀하게 통제하고, 특정 영역에서 이상 징후나 감염이 발견될 경우 신속하게 해당 영역을 격리할 수 있는 구조를 제공한다.

NGFW 는 조직의 네트워크 환경이 온프레미스, 클라우드, SD-WAN 등 다양한 형태로 진화하는 과정에서, 네트워크 보안의 중심축으로 기능한다. 애플리케이션, 사용자, 기기, 위치 등 다양한 맥락(Context)에 따라 정책을 집행해 조직 전체의 보안 수준을 근본적으로 높이며, 제로트러스트 원칙을 네트워크 단에 실질적으로 구현하는 기술적 기반이 된다.

최근에는 기존의 전통적 방화벽은 점차 단종되고, 침입방지시스템(IPS)이나 DDoS 대응, 애플리케이션 제어 등 다양한 보안 기능이 포함한 NGFW 또는 UTM(Unified Threat Management) 형태로 구축·제공되는 것이 표준이 되고 있다.

3. Macro-Segmentation (매크로 세그멘테이션)

Macro-Segmentation 은 조직 내부 네트워크를 논리적으로 구분하고 통제하기 위한 대표적인 네트워크 세분화(Segmentation) 기술로, 주로 SDN(Software-Defined Networking) 기반의 차세대 스위치와 같은 고도화된 네트워크 장비를 통해 구현된다. 기존의 네트워크는 대개 단일구성이나 소수의 경계로만 구분되었지만, Macro-Segmentation 을 도입하면 VLAN(Virtual LAN), 서브넷 등 논리적 단위로 네트워크를 세분화하고, 각 세그먼트 간 트래픽을 정밀하게 통제할 수 있다.

특히 SDN 기반 Macro-Segmentation 의 강점은 네트워크 정책을 소프트웨어적으로 정의·자동화할 수 있다는 점이다. 네트워크 관리자는 네트워크 장비의 물리적 위치나 하드웨어에 구애받지 않고, 어플리케이션·사용자·기기 속성에 따라 논리적으로 네트워크를 구분하고, 각 영역별로 정책을 적용할 수 있다. 이렇게 함으로써, 네트워크의 민첩성과 유연성, 가시성을 동시에 확보할 수 있으며, 네트워크 트래픽 흐름과 보안 정책 집행을 더욱 세밀하게 제어할 수 있다.

Macro-Segmentation 은 어플리케이션 영역까지 정책 통제가 가능하다는 점에서 기존의 VLAN 또는 물리적 경계 중심 네트워크 분할보다 한 단계 진화한 개념이다. 각 세그먼트 간 트래픽 흐름을 엄격히 제한하고, 인가되지 않은 접근을 사전에 차단할 수 있으므로, 조직 내 위협이 확산되는 경로(횡적 이동, Lateral Movement)를 효과적으로 봉쇄하는 첫 번째 방어선이 된다.

제로트러스트 아키텍처 관점에서 Macro-Segmentation 은 조직 내부 네트워크의 보안 수준을 크게 높일 수 있는 핵심 기술이며, 이후 보다 정밀한 Micro-Segmentation 단계로 확장함으로써 실질적인 내부 보안 체계를 완성할 수 있다. Macro-Segmentation 을 통해 구축된 논리적 경계와 정책 기반 관리는, Micro-Segmentation 으로 확장될 때 더욱 세분화된 보안 정책 집행과 네트워크 가시성, 자동화된 관리 효율성 등 조직 전체의 보안 역량을 높이는 중요한 기반이 될 수 있다.

4. Micro-Segmentation (마이크로 세그멘테이션)

Micro-Segmentation 은 기존 Macro-Segmentation 보다 한층 더 세분화된 보안 전략이다. 네트워크를 OSI 7 계층(Application 계층) 수준에서 업무, 사용자, 애플리케이션 단위까지 세밀하게 분리하고 최소 권한 원칙에 따라 접근을 제어하는 고도화된 접근 방식이다.

기존의 네트워크 세분화가 주로 IP 주소, 포트 기반, VLAN 등 물리적·논리적 경계에 머물렀다면, Micro-Segmentation 은 서비스·애플리케이션 간의 관계, 목적, 실질적 트래픽 흐름을 중심으로 논리적으로 네트워크를 분할한다. 이를 통해 조직은 네트워크 내부에서 발생할 수 있는 위협이나 공격자의 횡적 이동(Lateral Movement)까지 정밀하게 통제 가능하다.

Micro-Segmentation 의 구현 방식은 크게 두 가지로 나뉜다.

첫 번째는 네트워크 기반의 Micro-Segmentation 으로, NGFW(차세대 방화벽), ZTNA 등 네트워크 장비에서 사용자, 기기, 위치, 접근 애플리케이션, 트래픽 유형 등 다양한 컨텍스트 정보를 바탕으로 애플리케이션 또는 사용자 그룹 단위로 논리적 경계를 설정한다. 이 방식은 트래픽을 실시간으로 분석하고, 미인가 접근이나 이상 행위가 발생할 경우 네트워크 단에서 즉시 차단할 수 있다.

두 번째는 시스템(호스트) 기반의 Micro-Segmentation 으로, 엔드포인트(서버, 워크스테이션 등) 단에 에이전트(Agent) 또는 에이전트리스(Agentless) 방식의 전문 솔루션을 설치해, 각 단말/서버 별로 세분화된 보안 정책과 접근제어를 적용하는 방식이다. 이 과정에서 네트워크 연결 구조(토폴로지)를 시각화하고, 각 애플리케이션과 서비스 간의 실제 네트워크 트래픽 흐름을 분석해 자동으로 세분화 정책을 생성·관리한다. 최근에는 AI, 머신러닝 기술이 적용되어 네트워크 환경과 정책을 자동으로 최적화하고, 이상징후 탐지, 정책 추천 등 운영 효율성을 높이고 있다

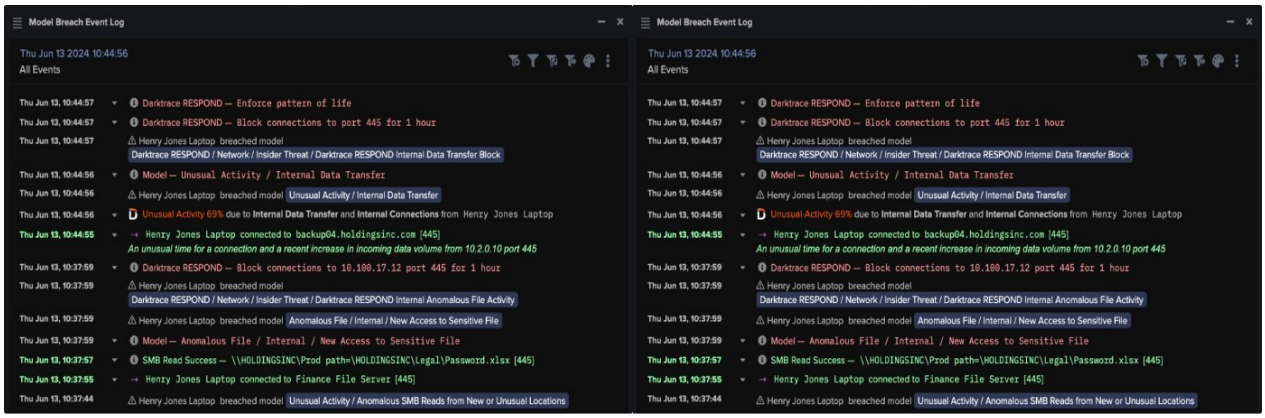
Micro-Segmentation 은 개념적으로는 네트워크 보안의 이상적 목표에 가깝지만, 실제 현업에서는 관리 복잡성·정책 설계 난이도 등 다양한 현실적 한계도 존재한다. 이에 따라 최신 솔루션들은 자동화, 가시성, 정책 추천 등의 고도화 기능을 중심으로 발전하고 있으며, 국내외 대기업·금융 등 다양한 현장에서도 실제 구현·운영 사례가 빠르게 확산되고 있다.

5. NDR (Network Detection and Response, 네트워크 탐지 대응)

NDR 는 제로트러스트 환경에서 네트워크 전 구간의 트래픽을 풀패킷(Full Packet) 단위로 실시간 수집·분석함으로써, 다양한 위협과 이상 행위를 정밀하게 탐지·대응하는 핵심 네트워크 보안 시스템이다.

NDR 의 가장 큰 특징은 단순 로그 수준의 이벤트 감지를 넘어 네트워크 내부와 외부를 오가는 모든 트래픽을 실제 패킷 단위로 저장·분석할 수 있다는 점이다. 이를 통해 알려진 공격 시그니처는 물론, 행위 기반의 이상 패턴, 비정상 통신, 의심스러운 파일 전송, C&C(Command & Control) 접속 등 폭넓은 위협 시나리오를 실시간으로 식별할 수 있다. 분석된 트래픽 데이터는 조직의 네트워크 토폴로지 맵을 자동으로 생성하고, 전체 인프라의 연결 구조와 트래픽 흐름을 한눈에 가시화하는 데 활용된다.

하지만, NDR 은 실무적으로 도입과 운영에 상당한 리소스와 전문성을 요구한다. 네트워크 전 구간에서 발생하는 대용량 트래픽을 실시간 저장·분석하는 인프라와 복잡한 룰셋, 세밀한 정책 설계가 필수적이며, 온프레미스·클라우드·IoT 등 다양한 환경 변화에 유연하게 대응할 수 있어야 한다. 그만큼 운영 과정에서 인력 부담과 시스템 복잡성이 높게 나타날 수 있지만, 최근에는 머신러닝과 AI 기반의 자동화 기능이 확대되면서 운영 효율성과 탐지 정확도가 크게 개선되고 있다.



출처 : DarkTrace, “Utilizing Darktrace Antigena (AI) for Automated”

그림 4. AI 를 활용한 네트워크 침해 분석 및 대응 / 네트워크 토폴로지 맵 생성

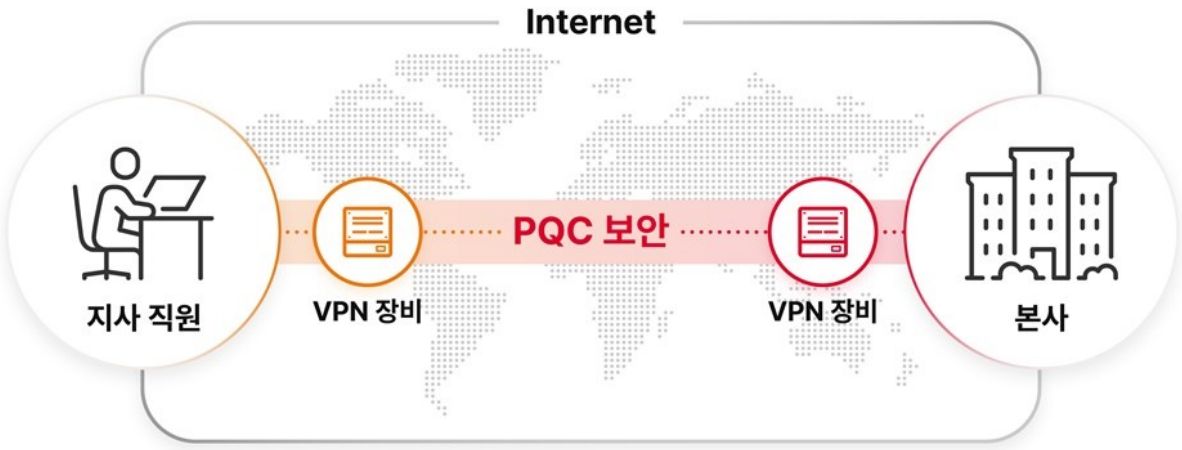
6. PQC (Post-Quantum Cryptography, 양자내성암호)

PQC 는 양자컴퓨터의 본격적인 상용화로 인해 기존 RSA, ECC 등 전통적 공개키 암호 알고리즘이 무력화될 가능성에 대응하기 위해 개발된 새로운 암호화 체계다. PQC 는 양자컴퓨터의 연산 능력으로도 쉽게 해독될 수 없는 수학적 난이도를 기반으로 설계되어, 장기적으로 네트워크·데이터 보호의 핵심 기술로 주목받고 있다. 최근 미국 NIST 에서는 ML-KEM, ML-DSA, SLH-DSA 등 세 가지 PQC 알고리즘을 표준으로 공식 채택했으며, 이를 기반으로 하는 암호화 기술이 점차 산업 전반에 확산되고 있다.

실제 PQC 솔루션은 양자암호통신장비(QENC/ROADM), 양자키관리(QKMS), 양자키분배(QKD) 등 다양한 형태로 구현되고 있다. 기존 VPN 을 대체하거나, 통신 구간 암호화, 인증서/키 발급·관리 등 보안이 필요한 다양한 인프라에 적용되어, 점진적으로 기존 알고리즘과 병행·대체되는 중이다.

제로트러스트 아키텍처에서는 네트워크, 데이터, 인증 등 조직 전반의 보안 체계에서 암호화가 핵심 역할을 하며, PQC 도입은 미래 환경 변화에 선제적으로 대응하기 위한 필수 전략으로 간주된다. PQC 기반 암호화는 외부 침입, 중간자 공격, 장기 보관 공격 등 기존 방식으로는 방어가 어려운 위협에도 내성을 갖출 수 있다는 점에서도 도입을 고려해볼 만하다.

네트워크 관점에서 PQC 는 기존 IPsec, SSL-VPN 환경과 동일한 사용자 경험과 정책을 제공하면서도, 양자컴퓨터에 안전한 키 교환 및 인증 구조를 구현한다. 이를 통해 조직은 장기적·미래 지향적 관점에서 안전한 통신 채널을 확보할 수 있으며, NIST 표준 PQC 알고리즘(ML-KEM, ML-DSA 등)을 활용해 기존 인프라를 대체하거나 하이브리드 방식으로 연동하는 것도 가능하다.



출처 : SK 텔레콤, "SKT-SKB, 국제망에 첫 PQC(양자내성암호) 상용화"

그림 5. PQC-VPN 개념도

다만, 현재 실무 환경에서 PQC 가 상용화되어 널리 사용되는 사례는 많지 않으며, 향후 양자 컴퓨팅 환경 도래에 대비하여 미리 검토하고 파일럿 적용 사례를 경험해보는 것이 필요하다.

네트워크 필러는 제로트러스트 아키텍처의 실질적 구현을 좌우하는 중심 축이다. ZTNA, NGFW, 세그멘테이션, NDR, PQC 등 다양한 네트워크 보안 시스템들은 각각의 기능을 넘어서, 조직 내 모든 트래픽의 흐름을 가시적으로 통제하고, 위험 요소를 선제적으로 탐지·차단하는 역할을 담당한다.

온프레미스와 클라우드, 본사·지점·원격 등 다변화된 업무 환경에서도, 네트워크 단에서 트래픽 흐름의 세분화, 실시간 정책 적용, 통합 가시성 확보, 위협 탐지·대응 및 암호화 등 다양한 요구를 충족할 수 있어야 한다. 이 과정에서 각 시스템은 단일 목적이 아니라 상호 연동을 통해 네트워크 전체의 보안 수준을 일관되게 유지한다.

네트워크 필러의 다양한 시스템의 유기적 연계를 통해 제로트러스트 환경에서 네트워크 신뢰성과 보안 수준을 안정적으로 유지할 수 있다.

■ 맺음말

제로트러스트 아키텍처가 본격적으로 주목받게 된 배경에는 온프레미스 환경에서 클라우드와 하이브리드, 그리고 원격·재택근무로 급격히 확산된 업무 환경 변화가 있다. 이런 변화로, 조직의 네트워크는 한층 더 복잡해졌으며, 공격 표면도 크게 확대되었다. 제로트러스트 환경에서 네트워크 필러는 변화하는 환경에 맞춰 조직 전체의 연결을 실질적으로 통제하고, 신뢰성 검증과 위협 대응의 중심 역할로 동작해야 한다.

네트워크 필러는 더 이상 데이터를 단순히 전달하는 물리적 기반이 아니라, 조직 전체의 연결 구조와 보안 통제를 실질적으로 아우르는 핵심 영역으로 진화했다. 모든 사용자의 접근, 디바이스의 연결, 업무 데이터의 이동, 클라우드·지점·본사 간 연계 등 디지털 환경의 모든 접점이 네트워크를 통해 구현되기 때문에, 네트워크 필러에서의 정책 집행과 신뢰성 검증은 곧 조직 전체의 보안 수준을 결정짓는 기준이 된다.

네트워크 필러의 본질은 단일 시스템의 도입이나 특정 솔루션 배치에 있지 않다. 네트워크 인벤토리, 흐름 분석, 트래픽 암호화, 접근 제어, 논리적 경계 설정, 세그멘테이션, 네트워크 가용성, 복원성, 모니터링, 리소스 관리 등 다양한 관리적·기술적 요소가 유기적으로 통합되어야만, 실질적인 보안성과 운영 효율성을 동시에 달성할 수 있다. ZTNA, NGFW, NDR, 세그멘테이션과 같은 주요 시스템들은 각자의 영역에서 중요한 역할을 하지만, 궁극적으로는 네트워크 흐름 전체의 신뢰성, 위협 탐지, 정책 적용이 일관되게 유지되도록 상호 연동·통합되어야 한다.

네트워크 필러의 이런 고도화된 기술적 구성과 운영 전략은 제로트러스트 아키텍처의 근본 원칙인 "신뢰하지 않고 항상 검증한다(Never trust, always verify)"를 실제 업무 환경에서 실현할 수 있는 토대를 마련한다. 온프레미스에서 멀티 클라우드, 본사에서 원격 근무자까지 다양하게 연결되는 복잡한 네트워크 환경에서도 지속적으로 신뢰성을 검증하고 실시간으로 보안 정책을 집행할 수 있게 함으로써, 조직은 외부 및 내부로부터의 보안 위협을 실질적으로 감소시키고 보안 대응력을 높일 수 있다.

결론적으로, 네트워크 필러는 제로트러스트 아키텍처에서 가장 근본적이고 본질적인 통제 축으로 동작한다. 네트워크 필러를 중심으로 기술적 연계와 통합 관리 체계를 강화하는 것이 향후 조직 보안의 실질적이고 효과적인 대응 전략이 될 것이다. 조직은 네트워크 필러의 지속적인 고도화와 정교한 정책 설계를 통해 복잡하게 진화하는 디지털 환경과 증가하는 사이버 위협에도 제로트러스트 기반의 견고한 보안 체계를 유지할 수 있을 것이다.

■ 참고 문헌

[1] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[2] NIST SP 800-215, “Guide to a Secure Enterprise Network Landscape”, 2022.11

[3] DoD, “Zero Trust Overlays”, 2024.06

[4] 국가사이버안보센터, “국가 망 보안체계 보안 가이드라인(Draft)”, 2025.01

■ 참고 자료

[1] SK쉴더스, “제로트러스트의 시작:SKZT로 완성하다” – 브로슈어

[2] Gartner, “Best Zero Trust Network Access Reviews 2025”

[3] Gartner, “Best Network Detection and Response Reviews 2025”

[4] IT데일리, “[ZTNA] 차세대 네트워크 보안으로 부상한 ‘ZTNA’ / 국내외 ZTNA 업체별 동향”

[5] DarkTrace, “The most advanced NDR solution, powered by Self-Learning AI”

[6] Cato Networks, “Zero Trust Network Access (ZTNA)”

[7] Paloalto, “What is Zero Trust Network Access”

[8] Fortinet, “Zero Trust Network Access(ZTNA) to Control Application”.

EQST INSIGHT

2025.07

SK 쉴더스

SK쉴더스(주) 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 SK쉴더스 EQST사업그룹
제 작 SK쉴더스 마케팅그룹